NRAC

Naval Research Advisory Committee Report

Technology for Base Security

March 2003

DISTRIBUTION STATEMENT C:
Distribution authorized to U.S. Government agencies and their contractors; Administrative/Operational Use, March 2003. Other requests for this document Shall be referred to the Naval Research Advisory Committee.

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

NRAC 03-2

COPY NO.

This report is a product of the United States Naval Research Advisory Committee (NRAC) Panel on Technology for Base Security. Statements, opinions, recommendations, and/or conclusions contained in this report are those of the NRAC Panel and do not necessarily represent the official position of the United States Navy and United States Marine Corps, or the Department of Defense.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
March 2003	Group Study	May 2002 - March 2003

4. TITLE AND SUBTITLE
Technology for Base Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
W.F. Weldon, E. Horvitz, J.A. Johnson, E.R. Kohn, M.J. Lister, W.A. Neal, J.Y. Rodriguez, K.A. Smith, T.B. Smith, R.C. Spindel, G.E. Webber

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Research Advisory Committee
800 North Quincy Street
Arlington, VA 22217-5660

8. PERFORMING ORGANIZATION REPORT NUMBER
NRAC 03-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Assistant Secretary of the Navy (Research, Development and Acquisition)
1000 Navy Pentagon
Washington, DC 20350-1000

10. SPONSOR/MONITOR'S ACRONYM(S)
ASN(RD&A)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement C: Distribution authorized to U.S. Government agencies and their contractors; Administrative/Operational Use, March 2003. Other requests for this document shall be referred to the Naval Research Advisory Committee.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Immediately following terrorist attacks on September 11, 2001, over 10,000 Naval Reservists were mobilized and were effective in establishing increased safeguards. A CNO Task Force concluded that technology was available that could be applied to enhance the effectiveness of current base security efforts and to improve the efficiency of manpower usage. The NRAC was charged to execute a study to "identify technology that can be applied to U.S. Naval and Marine bases to provide enhanced security for the bases while reducing manpower dedicated solely to security duties. The charge included the assessment of existing technologies as well as the identification of appropriate Naval science and technology investment. The study concluded that: 1) there are significant technology issues related to the testing of new technology, particularly implementation of commercial-off-the-shelf options; 2) there are recent advances in research suitable for quick product development; 3) there are important research issues regarding fusing of information from heterogeneous sources, multi-source, time-critical decision aids, and improving watchstander effectiveness. The Panel recommended implementing a technology based security system using a "Lead/Follow Base" approach. All new technology would be implemented and proven at a single lead base before being installed at other bases.

15. SUBJECT TERMS
Antiterrorism, Force Protection, RAPIDS, SOC, Security Operations Center, CAC, Common Access Card, Perimeter Security, Air Perimeter Security, Trusted Vehicles, Unverified Vehicles, Controlled Areas, Decision Aid, Virtual Visitor Center, Smart Card, Reduced Manning, Data Fusion

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dennis L. Ryan, III
UNCLAS	UNCLAS	UNCLAS	UNCLAS	74	19b. TELEPHONE NUMBER *(Include area code)* (703) 696-4875

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

This page intentionally left blank

Naval Research Advisory Committee Report

MARCH 2003

Technology for Base Security

DISTRIBUTION STATEMENT C:
Distribution authorized to U.S. Government agencies and their contractors; Administrative/Operational Use, March 2003. Other requests for this document shall be referred to the Naval Research Advisory Committee.

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

NRAC 03-1

COPY NO

This page intentionally left blank

Table of Contents

Documentation Page i
Executive Summary 3
Terms of Reference 5
Panel Membership 7
Briefing Outline 9
Sites Visited 11
Study Drivers 13
Aggravating Factors 15
Current DoD Decision Aid 19
Security Manpower 21
Base Security Problems 25
Approach 29
Technology for Perimeter Security 31
Approach for Air Perimeter Security 33
Outer Gate – Trusted Vehicles 35
Outer Gate – Unverified Vehicles 39
Inner Gate – Controlled Areas 41
Security Operations Center 43
Technologies for Security Operations Center 45
Implementation Strategy 47
Base Security Spiral Development 49
Conclusions 51
Recommendations 55
Appendix A – Terms of Reference A-1
Appendix B – Briefings and Visits B-1
Appendix C – CAC Cards and Biometrics C-1
Appendix D – Acronyms D-1

This page intentionally left blank

Executive Summary

Immediately following terrorist attacks on September 11, 2001, over 10,000 Naval Reservists were mobilized in support of Operations Noble Eagle and Enduring Freedom. Over fifty percent of the Naval Reservists mobilized provided increased security at Navy shore installations. This reaction, along with the use of manpower drawn from the Auxiliary Security Force and close cooperation with local law enforcement entities, was immediate and effective in establishing the safeguards recommended for Force Protection Condition (FPCON) DELTA. In the ensuing weeks the FPCON condition was lowered, first to CHARLIE, and then to BRAVO Plus.

The Chief of Naval Operations (CNO) subsequently requested a Task Force (TF) to assess the efficient utilization of Naval Reservists in meeting watchstanding requirements for FPCON BRAVO and CHARLIE and to compile and share best practices, lessons learned, and potential uses of technology. The TF concluded that technology was available that could be applied to enhance the effectiveness of current base security efforts and to improve the efficiency of manpower usage. They also concluded that: "In view of the pace of technology development, a frequent look at the balance between technology and manpower is warranted."

In May of 2002, the Naval Research Advisory Committee (NRAC) was charged to execute a study to "Identify technology that can be applied to U.S. Naval and Marine bases to provide enhanced security for the bases while reducing manpower dedicated solely to security duties." The charge included the assessment of existing technologies as well as the identification of appropriate Naval science and technology (S&T) investment.

The Study Panel membership included expertise in Navy and Marine Corps base operations, radar, sonar, sensors, artificial intelligence and automation of complex processes. Visits to Naval Station Norfolk, Naval District Washington and Naval Air Station North Island, among others, provided insight into the lack of coordination in developing enhanced base security after September 11, 2001. The panel participated in several fact-finding meetings and visits during June, July and August and then met for two weeks in October to complete the study. The results of the study were briefed to the Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RDA)) on 11 October 2002 and to the Commander, Fleet Forces Command (CFFC) on 29 October, 2002.

During the study the Panel realized that although base security throughout the world was important, the main drivers for the study along with some unique aggravating factors favored focusing the study on homeland bases exclusively. Of particular note were the realizations that many bases are proximate to densely populated areas and that rationale for and options to the use of deadly force were not well defined. With these premises in mind, the study priorities became: 1) reducing manpower requirements in all FPCONs; 2) providing secure rapid access for authorized personnel; and 3) improving base security, particularly by providing realistic decision making capabilities and increasing standoff distances from potential targets. The Panel then categorized the technologies applicable as to application to the land, sea, or air perimeters around bases. Research showed that there were a significant number of individual technologies that have promise for application to protect the land and sea perimeters. However, when it came to protection of the air perimeter, the Panel

concluded that technology alone could not solve the problem, political action is necessary. In all cases, the application of technology to replace manpower will require a solid command and control (C^2) element to function cohesively. Additionally, there is recognition of the need for substantial pursuit of improved collaboration and decision making tools. The Panel accordingly, described an approach for efficiently implementing new technology.

The specific conclusions of the study are that there many Department of Defense (DoD) security efforts currently under way or ramping up. However, there are political, programmatic, and budgetary issues that are impeding a coherent and effective implementation of these efforts. Additionally, there are significant technology issues related to the testing of new technology, particularly implementation of commercial-off-the-shelf options. On the plus side there are also some recent advances in research that may be quickly developed into products. Finally, there are important research issues that must be pursued: fuse information from heterogeneous sources; develop multi-source, time-critical decision aids; and improve watchstander effectiveness.

The Panel recommended implementing a technology based security system using a "Lead/Follow Base" approach. All new technology would be implemented and proven at a single lead base before being installed at other bases. It was envisioned that this could be done in three phases. The first phase would upgrade perimeter technology. The second phase would improve entry point (gate) technology. The final phase would then integrate the previous phases with the implementation of a Security Operations Center for C^2. In order to execute such an approach, an integrated project team is proposed.

Terms of Reference

- **Identify technology that can be applied to U.S. Naval and Marine bases to provide enhanced security for the bases while reducing manpower dedicated solely to security duties.**
  - **Review and assess the application of technology with respect to ... anti-terrorism/force protection (AT/FP) issues.**
  - **Review and assess current research and development of AT/FP technologies and recommend appropriate naval science and technology investment, both near and far term, to enhance base security.**

Naval Research Advisory Committee

Terms of Reference

Introduction

Immediately following terrorist attacks on September 11, 2001, over 10,000 Naval Reservists were mobilized in support of Operations Noble Eagle and Enduring Freedom. Over fifty percent of the Naval Reservists mobilized provided increased security at Navy shore installations. This reaction, along with the use of manpower drawn from the Auxiliary Security Force and close cooperation with local law enforcement entities, was immediate and effective in establishing the safeguards recommended for Force Protection Condition (FPCON) DELTA. In the weeks following September 11th the FPCON condition was lowered, first to FPCON CHARLIE, and then to FPCON BRAVO Plus.

The Chief of Naval Operations subsequently requested a TF to assess the efficient utilization of Naval Reservists in meeting watchstanding requirements for FPCON BRAVO and CHARLIE and to compile and share best practices, lessons learned, and potential uses of technology. The TF concluded that technology was available that could be applied to enhance the effectiveness of current base security efforts and to improve the efficiency of manpower usage. They also concluded that: "In view of the pace of technology development, a frequent look at the balance between technology and manpower is warranted."

In May of 2002, the Honorable John J. Young, Jr., ASN(RDA) charged the Naval Research Advisory Committee (NRAC) to execute a study to "Identify technology that can be applied to U.S. Naval and Marine bases to provide enhanced security for the bases while reducing manpower dedicated solely to security duties." The charge included the assessment

of existing technologies as well as the identification of appropriate Naval S&T investment. The complete Terms of Reference (TOR) for the study are included in Appendix A.

Study Panel Membership

- **Professor William F. Weldon - Chair**
- **Dr. Eric Horvitz (Microsoft)**
- **Dr. Joseph A. Johnson (Florida A&M)**
- **VADM Edwin R. Kohn, Jr (USN, Ret)**
- **Mr. Mark Lister (Sarnoff Corp)**
- **Dr. William A. Neal, M.D. (West VA. Univ)**
- **Mr. Joseph Rodriguez (Raytheon)**
- **Ms. Teresa B. Smith (Northrop Grumman)**
- **Dr. Robert C. Spindel (APL/U of Wash)**
- **LtGen Keith A. Smith (USMCR, Ret)**
- **Dr. George E. Webber (Getronics)**

- Mr. John M. Bachkosky (Systems Planning Corporation)
- Dr. Delores M. Etter (US Naval Academy)
- MajGen Paul A. Fratarangelo (USMC, Ret)
- Mr. Peter A. Gale (JJ McMullen Associates)
- Dr. James E. Hubbard (IproVica)
- VADM Douglas J. Katz (USN, Ret)
- Dr. James R. Luyten (Woods Hole Oceanographic Institution)
- Mr. James M. Sinnett (Boeing, Ret)
- RADM John T. Tozzi (USCG, Ret)
- Dr. Patrick H. Winston (MIT)

ADM Robert J. Natter, USN, CFFC Sponsor

CAPT Dennis L. Ryan, III, (USN, Ret) Executive Secretary

CDR Sue Fitzgerald, (USN, Ret) Assistant Executive Secretary

*** Summer Study Participants**

Naval Research Advisory Committee

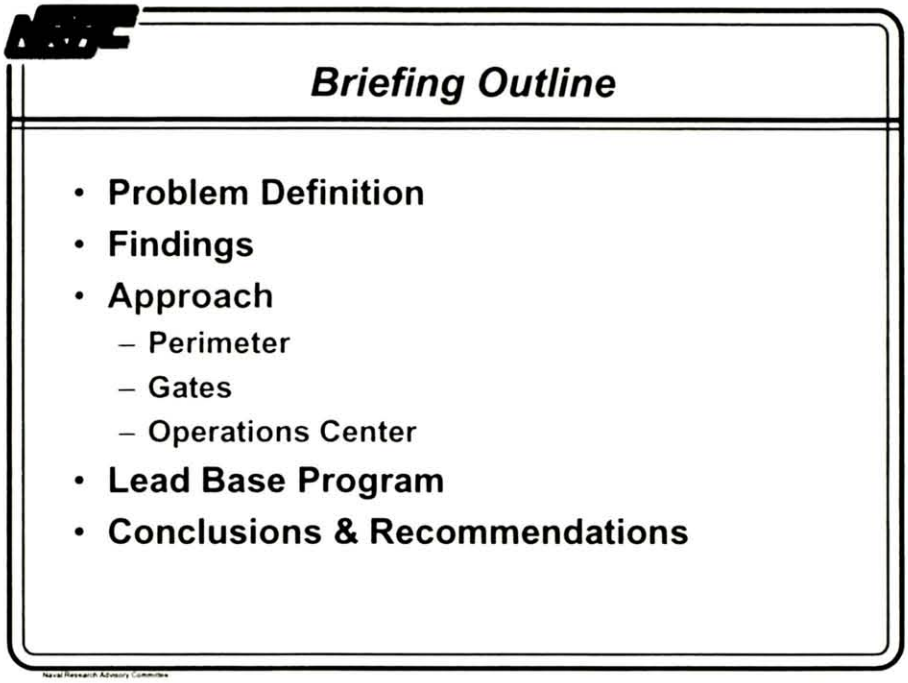
Study Panel Membership

NRAC study panels are typically composed of several NRAC members and outside experts recruited for the particular study. The recruitment and approval of outside experts for panel membership typically takes several months. In the case of this particular study, in order to respond quickly and given the general nature of the study, it was decided to undertake the study with a panel composed of the entire NRAC membership supplemented by a few preapproved adjunct members. During the course of the study, about half of the panel membership was split off to begin another study. The Technology for Base Security study was completed by the panel members indicated in bold face type in the above chart, but all of the panel membership shown contributed to the study.

Panel membership included expertise in Navy and Marine Corps base operations, radar, sonar, sensors, artificial intelligence and automation of complex processes. The Sponsor of the study was ADM Robert J. Natter, CFFC. Mr. Dennis Ryan served as Executive Secretary assisted by Ms. Sue Fitzgerald.

The panel participated in several fact-finding meetings during June, July and August and then met for two weeks in October to complete the study. The results of the study were briefed to ASN (RDA) on 11 October, 2002 and to CFFC on 29 October, 2002.

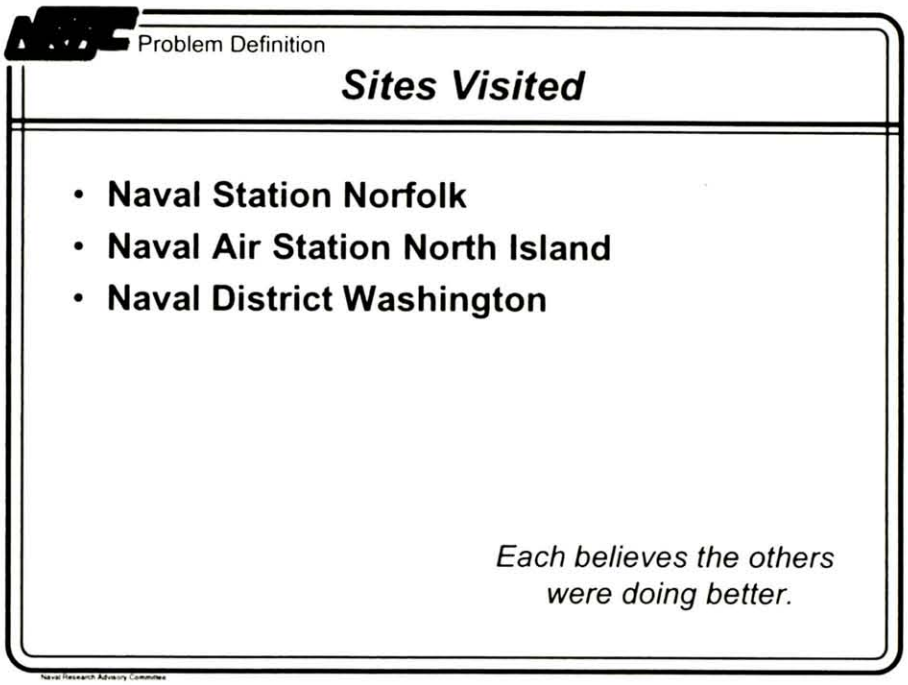
This page intentionally left blank



Briefing Outline

This report follows the format of an annotated set of charts from the briefings presented to ASN (RDA), CFFC and in the Pentagon Auditorium on 18 November, 2002. The first section of the report deals with the identification of problems associated with present base security system and their impact on manpower. The second section lays out the Panel's findings regarding these problems. The third section defines the Panel's approach to solving these problems. The fourth section describes a risk mitigation program for implementing the approach and the final section discusses the Panel's conclusions and recommendations.

This page intentionally left blank



Sites Visited

Visits to Naval Station Norfolk, Naval District Washington and Naval Air Station North Island provided insight into the lack of coordination in developing enhanced base security after September 11, 2001. Individuals responsible for base security at each site were generous with their time and openly discussed their own efforts to improve local security operations. Each confidently assured us that our questions and concerns would be resolved when we visited one of the other sites. This confidence that 'the problem was being taken care of elsewhere' was indicative of the uncoordinated, ad hoc way in which the Navy's base security needs were being addressed in the aftermath of September 11, 2001.

Visits to the DoD Common Access Card (CAC) program office and the Navy CAC program office provided the panel with information on the status within DoD of this critical technology as well as a time table for future upgrades.

A list of all visits and briefings presented to the NRAC panel is contained in Appendix B.

This page intentionally left blank

Problem Definition

Study Drivers

- 68 major stateside Naval bases vulnerable
- 5,000 reservists lost from security force
- Access by 1,000s of vehicles and 10,000s of people each day
- Significant security threats not addressed
- No alternative to effective base security
  - Lives lost
  - Remediation costs
  - Loss of Fleet capability

Study Drivers

The Study Panel focused their efforts on stateside bases because those bases were directly affected by the addition and subsequent removal of 5,000 reservists from their security forces. Further, those bases were judged to be the least prepared for the evolving terrorist threat. Maintaining a secure environment at these stateside bases is complicated by the need to provide access for thousands of vehicles and tens of thousands of people each day. Almost invariably, as the Panel visited bases, they learned of unprotected sections of the base perimeter and other security threats for which little or no provision had been made. To their credit, base commanders and security officers spoke quite candidly with the Panel about these deficiencies. Generally they were due to a lack of resources but in some cases there simply appeared to be no practical solution to the problem. These areas are covered in more detail later in this report.

In each facility visited, security personnel were aggressively improvising solutions to their security problems. While these efforts are laudable, they also reflect an absence of institutional focus on base security. In the light of recent experiences overseas, it is clear that there is no acceptable alternative to effective base security in terms of lives lost, remediation costs or loss of Fleet/Force capability.

This page intentionally left blank

Problem Definition

Aggravating Factors

- "Safe Haven" national mindset
- Proximity of high density civilian centers
- Short distances from base perimeter to critical areas
- Public access to bases
- Base consolidations with resulting concentration of high value assets
- Criteria for Use of Deadly Force

Naval Research Advisory Committee

Aggravating Factors

The difficulty of providing a secure environment at stateside bases is compounded by a number of aggravating factors. As a nation, we have enjoyed a long period of freedom from credible threats to our infrastructure resulting in a national sense of freedom and security. We have allowed high population density civilian centers to grow up surrounding and immediately adjacent to our most important stateside bases. Immediately following 11 September, 2001, base commanders quickly learned the negative impact that relatively minor changes in security procedures could have on nearby civilian activities. Increased gate security often resulted in traffic backed up for miles outside base gates.

In many cases, proximity of surrounding civilian activities has resulted in uncomfortably short distances from base perimeters to critical areas. This increases the difficulty of adequately protecting those areas. Base consolidations have resulted in high value assets being concentrated in fewer places (as reflected in the photo on the cover of this report), further compounding the problem. In an effort to be "good neighbors" and increase public understanding and support, public access to bases has been encouraged in ways ranging from bus tours to concerts. Those well intentioned public relations efforts are now recognized as possible vulnerabilities to terrorist penetration. (Conversely, they may also provide opportunities for identifying and observing terrorist agents)

Ironically, the very things that the Navy and Marine Corps do so well in their "conventional" roles are the most problematic in stateside base security; namely, command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and power projection. The C4ISR function is very weak. Even more consternating, the provisions for use of deadly force by sentries are, at best, ambiguous and confusing.

This page intentionally left blank

Problem Definition

Study Priorities

- **Reducing manpower requirements (All FPCONs)**
- **Providing secure rapid access for authorized personnel**
- **Improving base security**
  - **Increased standoff distances**
  - **Realistic decision making**

Naval Research Advisory Committee

Study Priorities

Seeking solutions to the stateside base security dilemma, the Panel chose to focus on three areas:

(1) Reduction of security manpower requirements under all FPCONs: Escalation from FPCON ALPHA to FPCON DELTA essentially doubles the manpower required to provide base security. Although most time is typically spent at lower FPCONs, it is essential that any technology employed provide equal or greater manpower savings at the higher FPCONs if real savings are to be realized. At higher FPCONS, base personnel are often required for other critical activities and diverting them to security duties means that these other activities will suffer.

(2) Secure, rapid access for authorized personnel: Every base commander interviewed by the study panel emphasized the importance of being able to get base personnel to their duty posts in times of crisis. Elevated FPCONs today result in additional base personnel being transferred from their normal duty assignments to augment the base security force and often result in substantial delays for all base personnel getting on base. To be effective, proposed technologies must facilitate getting base personnel to their duty stations as well as relieving the manpower burden of base security.

(3) Improved base security: In addition to reducing manpower requirements and improving access, the panel attempted to identify technologies to improve base security, particularly those technologies which would address the problem of short standoff distances from base perimeters to critical assets and those which would insure that appropriate information and guidance were available in a timely manner to support effective decision making by the individual base security forces.

This page intentionally left blank

Problem Definition

Current DoD Decision Aid

In a situation that requires your immediate action, do not wait for permission to fire, and do not wait to be fired on!

DEADLY FORCE IS AUTHORIZED ONLY UNDER CONDITIONS OF EXTREME NECESSITY WHEN:

1. **You must act to protect yourself or others from the imminent danger of being killed or seriously hurt; AND**
2. **Non-deadly force will not stop the threat; AND**
3. **Innocent persons will not be put at unnecessary risk.**

CAUTION If YOU do not understand the orders for your specific post and when to use deadly force, STOP and tell your CDO now!

YOU must decide when a person is putting you or others in imminent danger of being killed or seriously hurt. YOU must decide when deadly force is required.

When someone comes towards towards you on foot, in car/truck, or in a boat, you should consider using deadly force when you see them:

1. Aiming a deadly weapon; or
2. Refusing to obey warnings ; or
3. Breaching a security boat; or
4. Ignoring a security boat; or
5. Doing anything else that threatens imminent death or serious bodily harm.
6. These are examples. One of these actions alone may allow you to use deadly force; on the other hand, you may see one or more of these actions and decide deadly force is not required. You must decide based on what you see, your training, and your common sense.

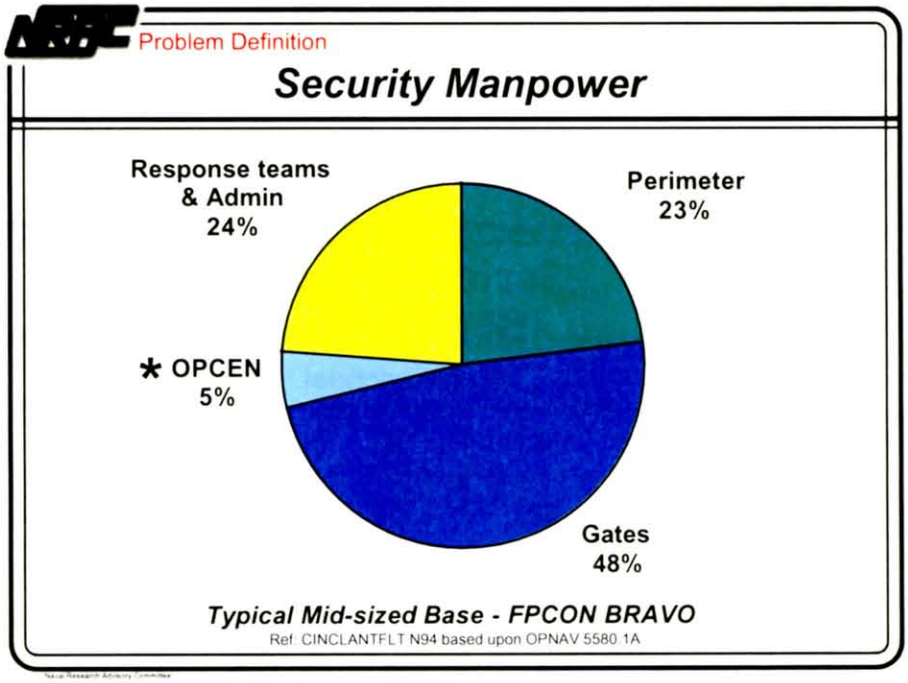
WARNING SHOTS ARE PROHIBITED IN THE UNITED STATES AND ITS TERRITORIES.

Naval Research Advisory Committee

Current DoD Decision Aid

This chart illustrates a pocket card, outlining DoD guidelines for use of deadly force, which is issued to base security personnel. The Study Panel was particularly concerned that this is indicative of forcing critical, life or death decisions to be made at the lowest level without adequate information or support. In particular, it is a result of the absence of an adequate C4ISR function in base security operations.

This page intentionally left blank



Security Manpower

Ensuring base security is a labor-intensive operation. In general, staffing requirements are based on minimums for response and access control. Office of the Chief of Naval Operations Instruction (OPNAVINST) 5580.1 Annex A provides procedures to determine Navy security department staffing requirements. The security staffing process detailed in the instruction enable Navy Activities, Claimants and Resource Sponsors to identify minimum staffing functions and capabilities at FPCON ALPHA (normal conditions). It also provides prioritized posting requirements. The primary duties of security forces, measured in man-hours, are entry screening (vehicle and pedestrian access control) and perimeter control.

The Panel found the following to be common practices in base security. Personnel entering a Navy facility are required to produce valid identification, which is visually checked by security force personnel. Cars are required to display a valid pass, and are subject to search using unaided vision for direct observation, and a mirror for searching under vehicles. Roving patrols frequently check the facility's perimeter looking for intruders or evidence of intrusion. Personnel in fixed, elevated posts often guard unfenced perimeters (e.g. beachfront, etc.)

The instruction also requires that, when feasible, security assets should be organized into a regional force structure to ensure the most cost effective and efficient security force. Determination of FPCON Alpha staffing requirements is based upon numerous factors that include: security patrol workload, access control point hours of operation and traffic volume, priority of afloat assets to be protected, administrative support requirements, and investigative workload. Determination of FPCONs Bravo, Charlie, and Delta staffing requirements is based upon specific capabilities and workload established for each protection measure. FPCON Bravo standards provide increased protection for off-base housing with a defined and controlled perimeter, surveillance detection teams for soft targets, vehicle inspection teams (to provide 50% coverage of all external access control points), increased

security patrols, escorts for personnel listed on the high-risk billet list, and increased pier, waterfront, and flightline security. FPCON Charlie standards add armed sentry and vehicle inspection teams (to provide 100% coverage of all external access control points), increased security patrols, and increased surveillance detection teams for soft targets. FPCON Delta standards add appropriately manned response and containment teams to respond and engage situations so that other patrols can remain in their assigned areas.

Security Manpower
Typical Mid-Sized Base

% of Personnel

FPCON	A	B	C	D
Perimeter	20	23	16	14
Gates	40	48	51	44
OPCEN	4	5	5	4
Other (MWD,CID, Admin)	36	24	28	38

Ref: CINCLANTFLT N94 based upon OPNAV 5580.1A

Naval Research Advisory Committee

Security Manpower (2)

The table above depicts the breakdown of security personnel assets at a typical mid-sized base for all Force Protection Conditions. Numbers are derived from the Security Staffing matrix as delineated in OPNAVINST 5580.1A. In Force Protection Condition Alpha (normal condition), a mid-sized base is allocated approximately 150 security personnel. Of these, 20% are involved in perimeter security. This category is made up of personnel manning mobile patrols that surveil the perimeter zones, buildings, magazines, and other vital assets. Forty percent of the total security force is located at access control points verifying identity of personnel and inspecting incoming vehicles. Four percent fill a command and control function in an operations center and the remaining 36% are involved in specialized functions (e.g. military working dog handlers, criminal investigative, administrative). When the FPCON increases to Bravo, twenty-one additional personnel are added to the security force. These personnel are used primarily to augment the various access control points where 100% identification of personnel is required, random vehicle searches are conducted, and all commercial vehicles are thoroughly inspected.

The pie chart, on page, 21 depicts security personnel breakdown at FPCON Bravo. Of approximately 171 personnel, twenty-three percent are conducting mobile patrols surveilling perimeter fences and boundaries, buildings, magazines and other vital assets. Forty-eight percent of the personnel are manning the various access points both at the front gates and into high value assets (e.g flightlines, piers). Five percent are manning a command

center while the remaining twenty-four percent are filling various other roles (high risk billet escort, military working dog, criminal investigative, administrative).

The charts very clearly depict that the majority of personnel, particularly in elevated force protection conditions, are delegated to manpower intensive jobs both in perimeter surveillance and access control. By introducing technology to perform all or portions of these functions, required manpower can be greatly reduced. Mobile patrols, while still required, will be used more for response, surveillance internal to the base, and protection of high value assets. Cameras, motion detectors, radars, and a variety of other equipment monitored by personnel in the command center can perform the majority of perimeter surveillance. Smart gates (to be described later) and chemical, biological, radiological, nuclear and explosive (CBRNE) sensors will greatly reduce the number of personnel manning access control points.

This page intentionally left blank

Findings

Base Security Problems

- **Overall**
  - **Standoff distances - time and range**
  - **Decision making**
    - **C4I integration**
    - **Connectivity with local authorities**
  - **FPCON ALPHA to DELTA doubles manpower** (Ref: OPNAVINST 5580.1A)
- **Land perimeter**
  - **Rapid base access for personnel**
  - **Vehicle searches manpower intensive**
  - **Trucks & bulk liquid carriers**
  - **Impact on surrounding operations**
  - **Unprotected perimeters**

Naval Research Advisory Committee

Base Security Problems

The next two charts list the findings of the Panel in terms of base security problems. Those problems shown in red are the ones the Panel found to be the most demanding. The combination of limited base size, geographic features, existing infrastructure and proximity of surrounding civilian facilities often make it impossible to protect critical assets by physically isolating them. The Panel worked to identify technologies that would address these limitations by effectively increasing the time and range over which critical security decisions could be made. The decision making process itself is probably the most neglected aspect of base security today. This study offers specific recommendations for supporting realistic decision making by integration of command, control, communications, computer and intelligence (C4I) functions including real time connectivity with other local authorities. Only by doing this effectively can timelines be extended and informed decisions be made expediently.

Security measures for the land perimeter of the base must make provision for rapid access of authorized personnel. Otherwise the inability of base personnel to reach their duty stations in times of crisis may render the effectiveness of the security system moot. Presently vehicle searches at points of entry are a major cause of delays and consume a disproportionately large amount of manpower (which increases further as FPCONs elevate). Fortunately this is one area where technology is available to substantially reduce manpower requirements and increase throughput. Trucks are more problematic than passenger vehicles because of their large volume, large number of packages carried and difficulty of access. High volume truck traffic (over 1000 per day at Norfolk) makes lengthy inspections unacceptable. Bulk liquid carriers (tank trucks) present an even greater security challenge since their construction and typical cargos make inspection even more difficult. To prevent impact upon proximate high density civilian activities the timely inspection of vehicular traffic is particularly critical.

Other portions of the base land perimeter that can be excessively demanding in terms of security personnel are those unprotected areas, such as beaches, where fencing may not be practical or does not exist. Fortunately, in most cases, security for these areas can be provided by technical means.

Findings

Base Security Problems (cont'd)

- Sea perimeter
  - Proximity of large ships / commercial traffic
  - Small craft
  - Swimmers
- Air perimeter
  - Private aircraft
  - Unmanned air vehicles
  - Commercial aircraft

Naval Research Advisory Committee

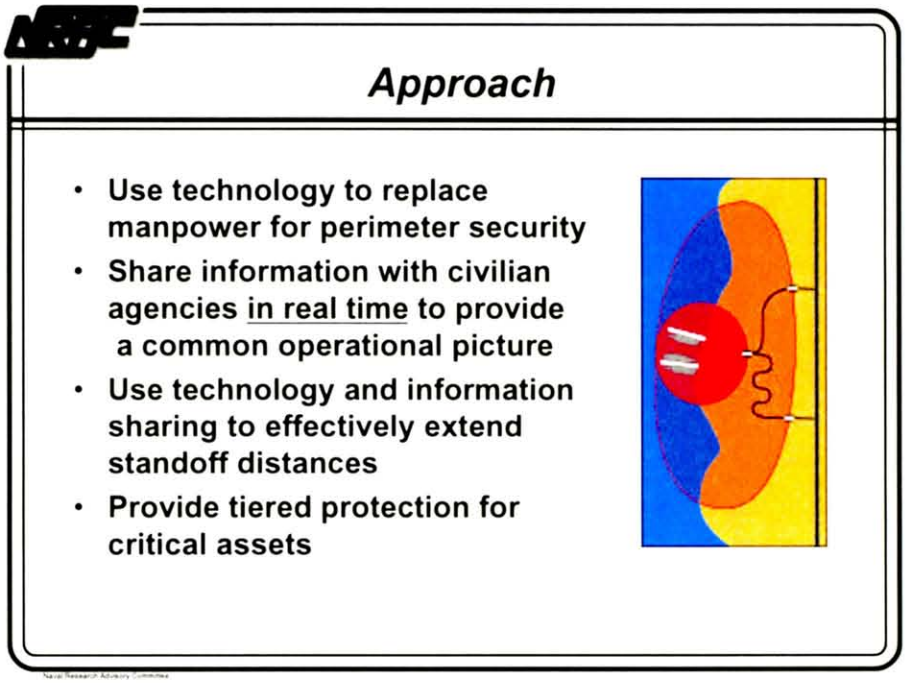
Base Security Problems (cont.)

The sea perimeter presents a more daunting security challenge than the land perimeter. Typically the Navy controls little of the surrounding water. The close proximity of large ships and commercial traffic presents obvious hazards, since cargos cannot be fully and accurately known and short standoff distances leave little time for response. In terms of response times, fast moving small craft present an even greater challenge and the large numbers of small craft in harbor locales make detection much more difficult. Swimmers too present a threat, although their limited speed and load capacity makes them less of a threat than boats. They do have the advantage of covert movement, but technologies to detect and neutralize them do exist.

The air perimeter represents the most difficult security problem. Air vehicles are, by far, the fastest moving threats and many Navy and Marine bases are near commercial or private airports where little or no tracking of air vehicles is done. The Federal Aviation Administration (FAA) has repeatedly refused to restrict the airspace over bases, even in cases where specific vulnerabilities are identified (such as weapons loading facilities). Commercial aircraft today probably present a lesser threat than they did before September 11, 2001 because of the more careful tracking of those aircraft. Private aircraft, which are subject to far less regulation than commercial aircraft, probably present the greatest security threat today. The growing availability of remotely controlled, unmanned aircraft, both military and commercial, represents a significant threat as well since such aircraft are completely unregulated and offer a combination of small size and low altitude flight that defies detection.

The difficulty of detecting and tracking air threats is compounded by the problem of dealing with them once detected. With the advantage of speed and altitude, an aircraft may

be able to hit its target even if its pilot or engine is disabled. Even destroying the craft may actually aid in the dispersion of a chemical, biological or radioactive contaminant. Furthermore, the difficulty in determining intent and the extremely short reaction times available once hostile intent is determined or assumed make defeat of air threats an extremely difficult problem.



Approach

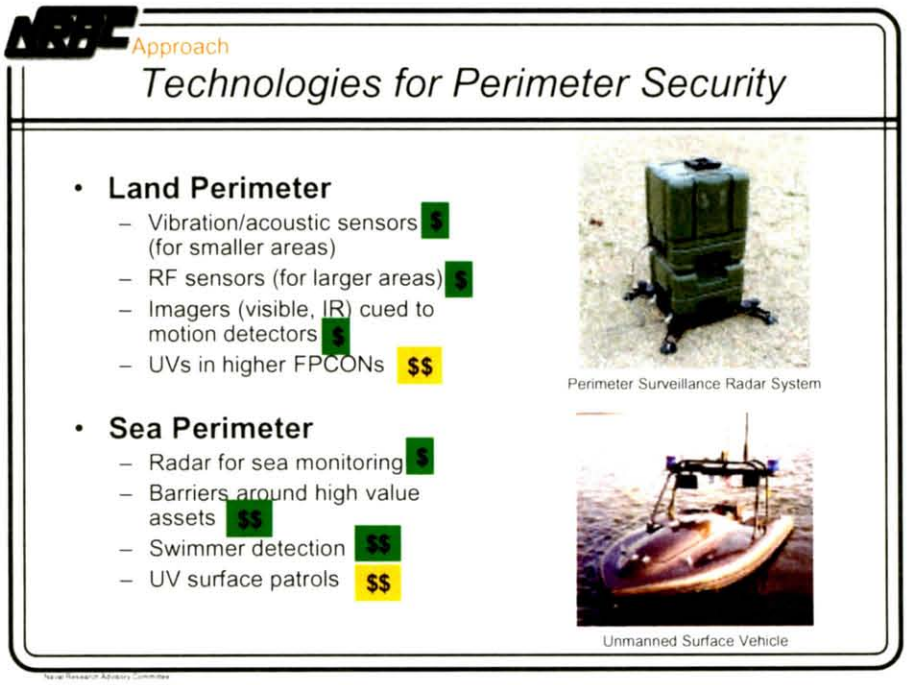
The Panel devised a fourfold approach to resolving the base security problem. The first is to utilize mostly existent technology to augment or replace perimeter security manpower. It is believed that, although an upfront investment will be required, the savings from reduced manpower requirements will more than offset the cost of this technology.

The rapidly evolving, well coordinated nature of terrorist driven events makes it essential to have a clear, complete and up to date understanding of what is occuring. Real time sharing of information with local authorities as well as regional and national authorities is essential.

The combination of suites of automated sensors around base perimeters and a common operational picture shared with other local jurisdictions can effectively increase physically short standoff distances by enabling predetermination of likely threats. By effectively extending the boundaries where pending threats are detected and classified, response times can be increased to more reasonable values.

Finally critical assets on a base (typically ships, aircraft, weapons storage areas and C4I facilities) can be further protected by a tiered arrangement of increasingly stringent security barriers. This tiered approach effectively increases standoff distances, provides more response time and addresses the problems of rapid throughput at perimeter gates with minimal impact on surrounding operations. It also clarifies the criteria for use of deadly force by providing more exclusive areas.

This page intentionally left blank



Technologies for Perimeter Security

Apart from use of intelligence to thwart terrorists before they approach base perimeters, the perimeters offer the first line of security against a terrorist attack. Sensors along these perimeters coupled with a Security Operations Center (SOC) will assist security forces in preventing terrorists from gaining access to a naval base whether by land, sea or air. The degree of difficulty is highest when dealing with the air perimeter and lowest along the land perimeter. Most sensors needed do exist, and performance enhancements to these sensors continue through DoD and commercial activity. The next two charts identify the appropriate sensor technologies for each of the three perimeters to be monitored. The colored box after each technology indicates two things. The color indicates the maturity of the technology (Green – commercially available, Yellow – exists in a laboratory, Red – requires research). The dollar signs indicate approximate cost ($ - low cost, less than $100,000; $$ - moderate cost, $100,000 to $1,000,000; $$$ - expensive, greater than $1,000,000)

Land Perimeter

A variety of sensors can be used to detect attempted penetration and cue a mobile force or remotely operated weapons. Vibration and acoustic sensors can be placed along a perimeter fence to detect activity. Radio frequency (RF) sensors (personnel/vehicle detection) will locate a person or vehicle approaching and/or penetrating the perimeter, and through the SOC automatically direct weapons or a strike force. Video cameras, operating in the visible, infared (IR) or millimeter wave spectrum with wireless connectivity can be placed strategically along the perimeter and cued by motion detectors or radars to track and classify the targets. All these sensors need to be fused and integrated by the SOC to focus on the potential threats while reducing the manpower required at the command center.

Unmanned ground vehicles (UGVs) with sensors and weapons can provide utility along the perimeter. How and when to use them needs to be studied in conjunction with the

perimeter sensor suite which can be easily deployed and moved using wireless network connectivity. The concept of tiered security applied to high value assets can also use the same sensors at the inner perimeters.

Sea Perimeter

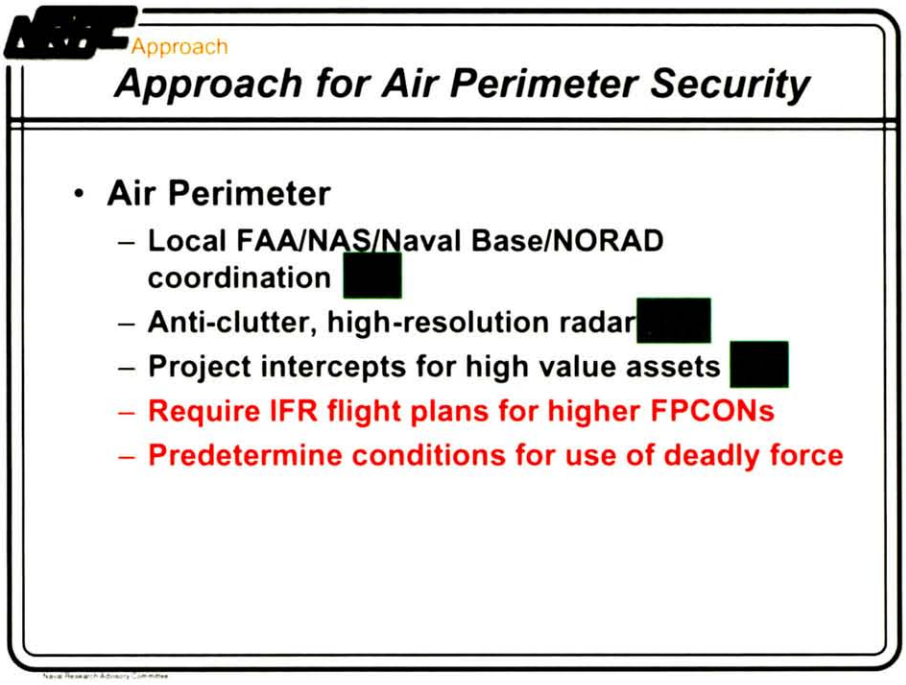
This perimeter presents a more challenging set of issues. Bases like Naval Station Norfolk and Naval Air Station North Island have a large concentration of high value assets and a limited seaward stand off distance. Small, medium, and large ships present a most difficult potential threat because they pass within 100 to 200 yards of moored naval ships, including concentration of aircraft carriers and submarines. Determining intent and response is the first issue. Where radar is not already available, one needs to be supplied and installed to detect and track water surface traffic. The output of this radar will be input to the SOC during the recommended third phase of the base security system development where algorithms can be used to help determine intent.

Pneumatic barriers can be installed around high value assets. Using the radar to determine bearing and speed of a ship, barrier penetration location can be predicted. Weapons (non-lethal or lethal) can be strategically placed and automatically directed to the predicted penetration point. Concept of Operations (CONOPS) needs to be established to determine the type of response as a function of threat scenarios. Once a ship turns into the barrier, response times become short, automation will be required and with medium to large ships, momentum may be impossible to impede.

Large ships need to be classified long before they enter the waterway and may require armed personnel to board a ship along with the harbor pilot. This is being done in San Diego with success. The medium sized and smaller fast boats also create a serious problem. Detection, tracking and determining intent in order to automatically train a defensive weapon is only a partial solution. With only 100 to 200 yards range required, the weapon size and its effectiveness need to be considered. Lethal and non-lethal weapons need to be examined to determine the best solution for each installation and threat type.

Swimmers present a lower level threat and can be detected with a variety of sonar systems. Sonar detections can then be used to cue video cameras via the SOC and to classify the swimmer or swimmers. Response times for this potential threat should be adequate.

As with the land perimeter, unmanned surface and underwater vehicles could patrol inside the pneumatic barriers but their utility should be studied with respect to their effectiveness versus easily deployed dockside sensors.



Approach for Air Perimeter Security

The air terrorist threat presents the most difficult problem and a satisfactory solution has eluded this Panel. Although there are radars to detect air traffic on some Naval bases, and also in some cases the air traffic picture is combined with inputs from FAA air traffic control, the current system cannot see small targets below 500 feet. In addition most small private aircraft operating under Visual Flight Rules (VFR) don't have transponders (and even if they did, a terrorist could turn them off as was done on 9/11/01). Sophisticated radars with anti sea and land clutter capability, installed a few thousand feet above the base or in an aircraft/UAV to detect and track low fliers, would be the only solution to identifying this threat

In order to develop potential solutions and actions, it is necessary to have a clear picture of the air situation around the base. Radar can detect air targets near or approaching high value assets. Tracking these targets to determine speed, bearing, and altitude is also essential. This capability doesn't exist today at the Naval Bases visited, but the technology is available. The indigenous radar must also have the ability to track a scintillating radar return as well as a transponder. A common operating air picture can be developed with inputs to the SOC from the FAA and the Naval Base radar. Algorithmic filters can be applied to only track potential threats, providing direction, speed, and altitude which can be used to project intercepts with high value assets. Weapons can be automatically directed, but the conditions under which they can be used are unclear at present. Threat aircraft carrying "dirty" radiological, chemical, or biological devices may do as much damage exploding in the air as in an impact detonation. In addition most Naval installations are surrounded by large civilian concentrations where falling contaminated debris could create major problems.

Many of the actions that can be considered have political connotations. Consider for example, limiting potential threats by suspending VFR flights over bases during high FPCONs, or allowing use of deadly force under FPCON Delta conditions. Neither of these actions are allowed today. Other actions to consider include grounding all private aircraft

traffic during high FPCONs (a political issue), the use of UCAVs around the base to collect/send data, and be capable of firing an air to air missile (an expensive weapon system). A high resolution side-looking radar on the UCAV could provide a detailed surface picture which could be integrated with other sensor inputs at the SOC. Sensors and technology are available to provide an integrated air and surface threat assessment, but are expensive and actions to eliminate threats once identified are presently undetermined. Establishing the rules of engagement to fire lethal or non-lethal weapons is an issue not addressed by this study. Air perimeter security solutions are difficult, politically charged, and require careful development.

Approach

Outer Gate - Trusted Vehicles

- **Vehicle ID and verification**
  - Valid vehicle tag (retro-reflective bar code) [redacted]
  - Vehicle reference image [redacted]
  - License plate recognition and correlation [redacted]
  - Undercarriage image [redacted]
- **Occupant ID and verification**
  - DoD proximity CAC [redacted]
  - Locally issued "smart card" for commercial vehicles (digital signature and PIN) [redacted]
- **Rapid deployment barriers for "rogue" vehicles** [redacted]

Outer Gate – Trusted Vehicles

Current procedures for securing physical access at gates are perhaps the most manpower intensive of all of the responsibilities of the base security staff. Entry gates currently comprise forty-eight percent of a typical base's overall security manpower requirements. Therefore this study has expended considerable effort in determining how new, but proven technologies and automation techniques can be used to more effectively automate gate security functions and thereby reduce manpower requirements and operational costs. The fact-finding conducted by the Panel in reviewing base security operations at several sites and in assessing a variety of emerging commercial technologies resulted in recommendation of an operational "smart gate" concept which leverages new technology and modified operational procedures.

The principal technology recommendations for the smart gate include:

- Implementation of DoD CAC at all entry gates - Smart cards are now becoming prevalent in the world and are being used for ID validation in industries from banking to commerce. There are a variety of different features, including biometrics that these cards incorporate for secure identification and access control. With the CAC, DoD currently has smart card technology. The CAC is registered to specific users and certified with fingerprint information. The DoD CAC accommodates several forms of data storage. The first of these is printed information, which includes picture, name, rank, grade and issue and expiration dates. It also incorporates a tamper-proof random access memory (RAM) and integrated circuit processor for storing and processing Public Key Infrastructure (PKI) public/private keys and X509 certificates and other application related data. Magnetic stripe technology is used for storing U. S. DoD, Security Enterprise

Integration Working Group (SEIWG), {SEIWG-012, Prime Item Product Function Specification for Magnetic Stripe Credentials} credential numbering descriptors, and both one-dimensional and two-dimensional bar codes are incorporated for local applications. In addition to these features, the DoD CAC office plans to add improvements and enhancements as technologies mature, including biometrics. The DoD Biometrics Management Office will play an important role in determining the specific biometrics that will be incorporated into the card. The first set of CAC biometrics capabilities to be deployed will be fingerprint biometrics. (see Appendix C)

The use of the DoD CAC technology at the entry gates can provide added security, increase throughput and reduce gate security personnel requirements. A large investment has already been made in this area and for interoperability reasons the Navy needs to transition to the use of standard DoD CAC for physical access controls. The Panel recognizes that there will necessarily be a transition period during which both DoD standard CAC cards and older legacy magnetic stripe ID cards will need to be accommodated. Low cost multiple technology card readers are currently commercially available to accommodate this transition.

- Use of visible imaging sensors with automatic feature recognition technology at gates can be used to correlate known reference information with point-of-entry information. In this case, an example is the use of license plate readers which identify vehicles and correlate information against base registration information as well as stolen vehicles databases provided by external agencies.

- Locally managed "access control lists" in a central database will allow rapid processing and correlation of in-coming information and determination of valid access. An example of such a database usage would be reading the CAC magnetic stripe /PIN information at a gate entry and correlating this information against a local access control list to determine if a person is cleared for entry. It is important that "access control list" data bases be managed by the local base-level security personnel, so that area and building accesses have the highest degree of responsiveness to local security conditions.

- Use of a highly automated "virtual visitor center" area for processing certain types of visitors would speed entry and potentially eliminate numbers of security personnel. This "virtual visitor center" would make extensive use of ATM-like interactive terminal technologies with automated ID card readers and imaging sensor technology. Imaging and audio interfaces would be provided to remote security operators. Actual interactions with human security operators would only be required on an "exception" basis for those cases where visitor ID and authenticated visit request information could not be verified autonomously.

In addition to smart gate technologies, the panel also recommended that new base/gate operating concepts be implemented to optimize traffic flows and enhance security. The proposed concepts would involve separating gates based on type of vehicle and risk. First gates would be segregated by vehicle type with separate gates for suppliers/vendors in commercial vehicles versus gates for personnel (employees, contractors, visitors, etc.) in smaller vehicles or walking onto the base. Traffic flows in each of these two sections would

be partitioned further based on risk. Specific access lanes would be provided for pre-verified or "trusted" vehicles/personnel versus unverified visitors. Unverified visitors would be processed using an automated, "virtual visitor center" concept based on risk and processed through special turnstile access areas. Once traffic cleared the outer gate areas, inner gates would be used to protect controlled areas or high value assets in a tiered security design. Inner gates could implement many of the same outer-gate technologies with added security identification and verification features

Gate separation and processing scenarios and respective technologies are described in more detail in the following paragraphs. The gate areas specifically discussed below are:

- Outer Gate – "Trusted Vehicles"
- Outer Gate - Unverified Vehicles
- Outer Gate - "Walk-ons" and Visitors
- Inner Gate - High Value Areas

Outer Gates-"Trusted Vehicles" - Fast Access

The smart gate functions would be slightly different for the outer perimeter (lower risk) gates where traffic volumes are greater as opposed to the inner perimeter (higher risk) gates. The outer gate functions will first be described in terms of vehicle control functions for pre-verified or "trusted" vehicles and secondly for unverified vehicles. As noted before, there would be separate gates for commercial vehicles versus small vehicles, however, the procedures for pre-verified "trusted" vehicles and unverified vehicles would be similar. It is expected that in most cases the vehicle flow rates will be highest for the small vehicle gates and therefore vehicle approaches would be clearly identified and separated into so-called "fast access" lanes for pre-verified vehicles with authorized occupants, and separate lanes for unverified vehicles and occupants.

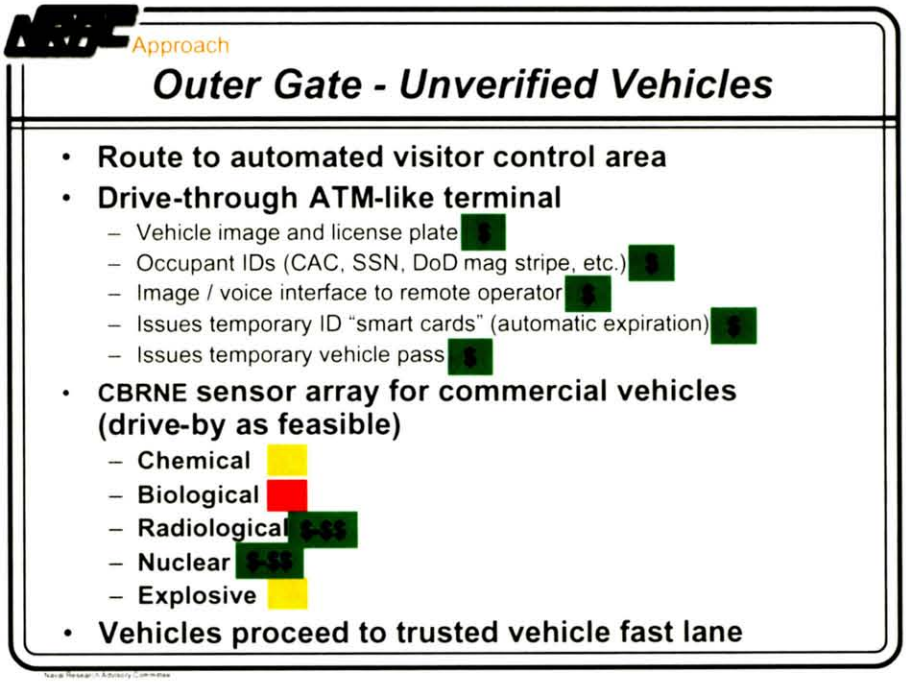
Vehicles in the "trusted" access lanes would be required to possess a vehicle tag issued by Base Security which would be clearly displayed, probably on the windshield or the front bumper, and would have an infrared (IR) retro-reflective bar code identification. This bar code would be automatically read at a distance by an automated reader on the gate as the vehicle approached. The bar code identification data would be instantaneously relayed to the central data base for correlation with current reference data on the vehicle and a registration reference image of the vehicle would be instantaneously returned to the gate guard's display for his quick visual check.

As the vehicle stops momentarily at the gate all occupants would be required to present their DoD proximity CAC cards which would be remotely read by the CAC smart card reader. This currently operates up to a distance of about 30 cm but the range will be extended with future versions of the card. It is expected that not all individuals will initially have CAC cards, therefore a multi-function reader will initially be used so that the older magnetic stripe ID cards can also be read (until they are transitioned out). Under higher threat conditions, vehicle occupants may be required to enter PIN and biometric data as well.

Verified visitors (verified by the process described in the next section) would be issued a temporary smart card which would meet the CAC card specification and be compatible with the CAC readers but would be locally issued and registered in the local reference data base on a temporary basis only. These visitor smart cards would contain

visitor data including picture and personal information, and local contact information, and would include automatic expiration features.

The trusted vehicle access lanes would utilize "pavement view" imaging cameras which would be able to automatically read and derive license plate information for real-time correlation with the remote central database and would also collect vehicle undercarriage imagery for real-time display to the gate guard as the vehicle approaches. A low-cost piezoelectric pressure sensor plate would also be deployed in the access lane so that the vehicle could be quickly weighed for correlation with the reference vehicle weight information which would have previously been recorded when the vehicle was originally registered. Rapid deployment physical barriers would be used at each of the fast access trusted vehicle lanes to effectively stop "rogue" vehicles.



Outer Gates- Unverified Vehicles

At both gate types (i.e. small vehicles and commercial vehicles), unverified vehicles which do not have a valid vehicle tag and/or contain unverified occupants would follow signs and be routed into an automated visitor control area. This "virtual visitor center" would make the maximum use of automated ID card readers, imaging sensors, and automated vehicle weight sensors. Vehicles would be directed into processing lanes where the operator would interface with ATM-like terminals without being required to leave the vehicle. Occupant ID cards would be presented to a multi-function card reader at the terminal. This card reader would accommodate the standardized DoD CAC cards as well as legacy magnetic stripe ID cards and also commercial magnetic stripe credit cards. Keyboard interfaces would be provided for PIN and other required data entries. Using one of these forms of identification, occupant IDs would be automatically established and checked against any pre-entered visit request and authorization information. As much as possible, all of these transactions would be automated, interactive transactions with the vehicle occupants. Direct interaction with a remote human security operator would only be required on an "exception" basis when either IDs could not be established automatically or when automated authorization checks failed. The remote security operator would interface with visitors using real-time imaging and voice interactive technology.

At the same time that the occupants are being verified for entry, their vehicle would be automatically imaged in order to collect license plate information and to provide a reference image of the vehicle for storage and later use. The vehicle would also be weighed using a low cost piezoelectric pressure sensor plate embedded in the vehicle lane. This data would be appended to the reference data file for this vehicle and automatically transferred to the central database at the base SOC. License plate information would be automatically

checked against stolen vehicle data cached at the local SOC database and periodically updated from external agency databases. For commercial vehicles, in addition to the information to be collected as described above, the vehicle would also be required to proceed through a CBRNE sensor array ("sensor tunnel") which would do an automated sweep to detect any low level nuclear radiation, as well as any low level chemical and biological trace indicators.

In the case where all of the above described identifications, checks and authorizations were successfully passed then temporary retro-reflective, vehicle tags and occupant temporary visitor ID smart card would be issued by the interactive ATM-style terminals. For commercial vehicles required to pass through the special sensor array, the vehicle tags and temporary occupant ID smart cards would be not be issued until after the sensor scans and this would be done at an exit terminal. When a vehicle and its occupants had received appropriate temporary vehicle tags and personal ID smart cards, they would then be directed into the "trusted vehicle" fast-access lane which has already been described.

Outer Gates- "Walk-Ons"

Access control for individual "walk-on" personnel would also be separated into entry "fast-access" for pre-verified or "trusted" personnel and separate access control processing for unverified visitors using the 'virtual visitor center" concept already described. Pre-verified or "trusted" personnel would be directed to proceed to a "smart turnstile" which would incorporate multi-function ID card readers and would enforce flow control. The multifunction ID card readers would accommodate the CAC smart cards as well as the legacy magnetic stripe ID cards until they could be phased out.

Unverified visitors would be directed to ATM-like terminals which have already been described and which would provide the visitors interface to the base's "virtual visitor center" functions. The terminal would accommodate CAC smart cards, legacy ID cards as well as commercial credit cards. It would also provide keyboard interfaces so that other information could be entered including drivers license information. Visible cameras incorporated into the terminals would record a photo record of the visitor for entry into the central database and for printing on the temporary visitor smart card. Once automatic visitor identification has been established verification checks would be made with pre-entered visit request and authorization information, and other correlations would be made with other information derived from national criminal databases and other sources. Once the visitor is successfully identified and authorized, then a temporary visitor ID smart card would be automatically issued at the terminal. This temporary smart card would be readable by the "smart turnstile" and would contain information describing the visitor, the areas and buildings for which he is authorized access, and would also incorporate automatic expiration features. At this point, the newly verified visitor would then be directed to proceed to the "smart turnstile" fast-access entry.

As before, it is expected that the transactions between the visitor and the "virtual visitor center" will be automated interactive transactions and will not require human interaction by the remote security operator. In those cases where the automated interactions fail, then camera imaging and audio interfaces are provided at the terminal to support the direct human-to-human interactions which may be required.

Approach

Controlled Areas

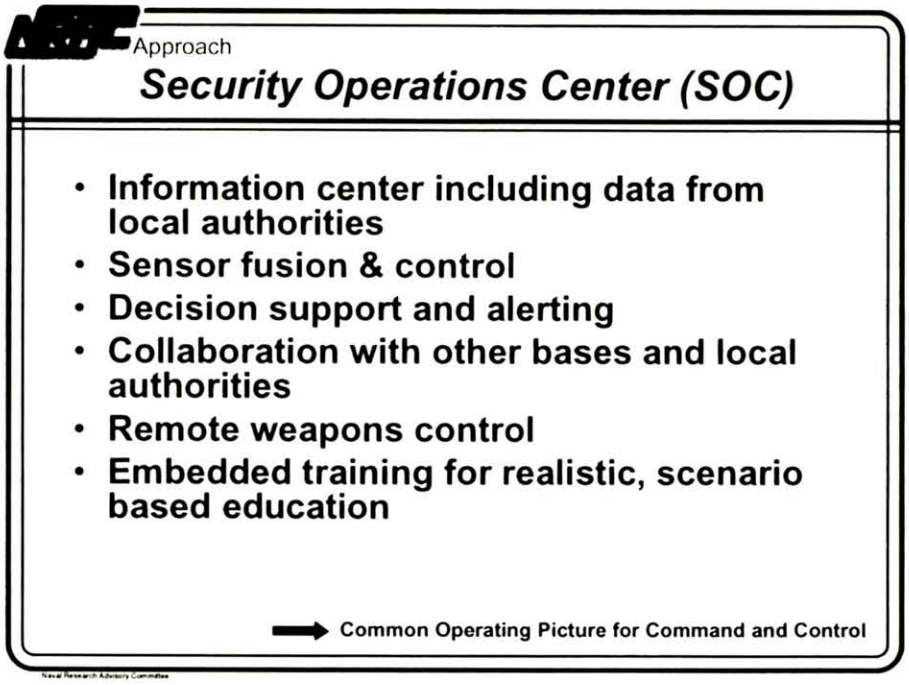
- **Increased stand-off distances**
  - Labyrinthine approach where possible
  - Second tier sensor scanning
- **Controlled area access control**
  - Inner gate
    - CAC card with biometrics [redacted]
    - Gamma ray scanner [redacted]
  - Perimeter: visible, IR, and vibration/acoustic sensors
- **Use of Deadly Force**

Inner Gates- Controlled Areas for High Value Assets

Inner gates will provide access for both personnel and vehicles into perimeter controlled areas containing high value assets. These high value assets are those things/areas, which as a result of a base-level vulnerability analysis, have been deemed to require higher degrees of security control and protection than that required at the base's outer perimeter access control gates. At these inner gates, vehicle occupants and "walk-ons" would be required to present appropriately pre-validated ID cards for automatic reading by a multi-function card reader. These would include the DoD proximity CAC smart card, a temporary visitor smart card authorized for area entry, or an authorized legacy magnetic stripe ID card. Additional verification of the proper binding between the ID card and the individual would be accomplished at the inner gate through the use of PIN entry and authentication as well as thumbprint biometrics. As a result, the multi-function card reader would be configured to incorporate thumbprint reading in accordance with the DoD Version 2 CAC card specifications and would optionally add additional biometrics as they were incorporated as part of the DoD CAC program. As these biometric functions are added, they would also be incorporated on the locally issued temporary visitor smart cards since these would be procured to meet the same card specification as the DoD card although they would only be temporarily registered at a local base level. As with the outer perimeter gates, reference photo images of the personnel involved would be displayed to the gate guard for quick manual comparison.

Vehicles intending to pass through an inner control gate would be required to display an authorized vehicle tag incorporating a retro-reflective infrared (IR) bar code. This vehicle bar code can be remotely read as the vehicle approaches the gate. Vehicle access authorizations are automatically checked remotely in real-time using the reference data base

at the SOC. These automated checks could be extended to not only include access authorization checks, but could also be set up to check time limits on when the vehicle was expected to transition from the outer gate to the inner gate. At the same time reference imagery of the vehicle is pulled from the database and displayed to the gate guard, the vehicle's undercarriage image originally captured at the outer gate would be retrieved from the database and displayed to the gate guard for his review. It is also expected that gamma ray imaging sensor arrays would be deployed at the inner gates so that vehicles, including bulk container trucks, could be reviewed for explosives and other threatening objects. Finally, low cost piezo-electric pressure sensing plates would be incorporated into the vehicle access lanes so that the vehicle can be quickly weighed and compared to its reference weight. Because the traffic flow rates at the inner gates are expected to be considerably less than those at the outer perimeter gates, additional time is available to conduct more extensive threat sensing including gamma ray imaging as a means of protecting high value assets. As with the outer perimeter gates, rapid deployment barriers such as wedge barriers would be deployed in the pavement in order to stop "rogue" vehicles.



Security Operations Center (SOC)

Effective utilization of base security assets requires a central C^2 function. The SOC is the facility to serve this function. The SOC with its inherent capabilities will need to be developed, implemented, and enhanced over time. Following certain design principals will help control costs (both development as well as operations and maintenance), ease technology insertion, facilitate interoperability, and maximize return on investment. The creation of the SOC needs to start with an overall systems analysis and architecture definition to identify the hardware and software requirements. Well managed systems integration will ensure components and subsystems will function together effectively thus preserving quality of collected data, personnel workload efficiency, and overall SOC effectiveness.

Another critical design principal is the definition of the interfaces required between the various subsystems of the SOC. Commercial standards should be employed as much as possible. This approach will help maintain configuration control and interoperability as SOCs are created at various bases. Also this commercial practice will facilitate plug and play capability.

The most valuable asset of any SOC will be the personnel. With the abundance of data and information available within the SOC and the operations tempo during crises, great care must be given to manage the human workload. Human factors analysis, included in the initial design, will help ameliorate workload issues. In order to maintain effective use of security personnel and speed quality decision making, constant diligence must be paid to the subsequent human factors design.

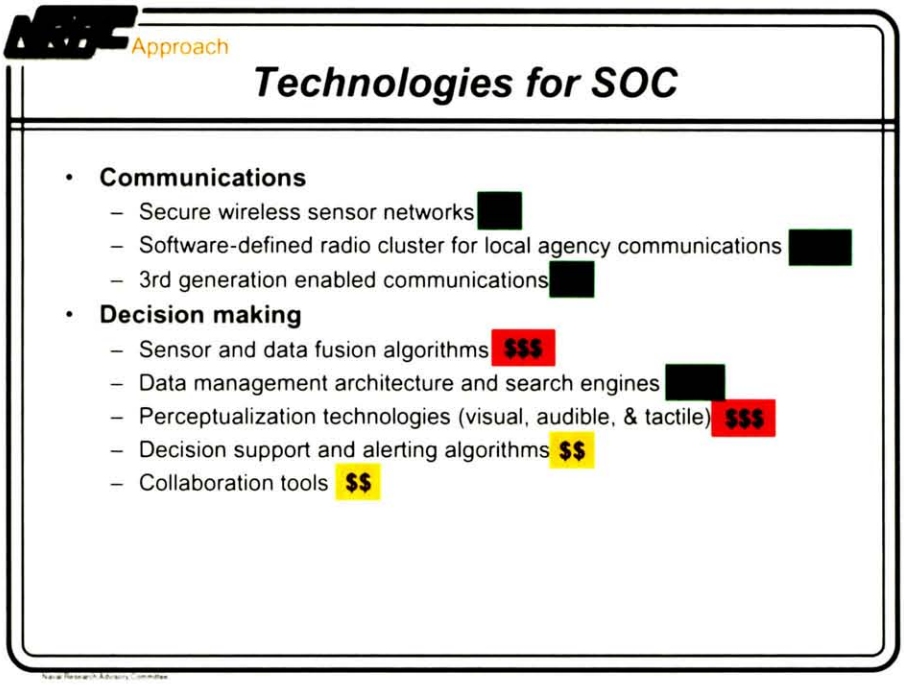
Finally, embedding training tools and capability into the SOC will facilitate realistic, scenario based learning. Data from events can be recorded and replayed to test various courses of action. Experts can employ real data and information sources to train less experienced personnel quickly, in situ.

There are a myriad of functions to be performed within the SOC. The Center will be the central location to receive, access, process, and fuse data. The sources of these data will include (but are not limited to) data from organic sensors on or around the base, real-time data from local authorities, and data available in a variety of databases. Example databases could be stolen vehicles, aliases, daily visitor logs, base personnel, etc. The SOC will have the ability to control various sensors on or around the base. This will empower security personnel to collect the data they require, when they need it, to make more informed course of action decisions.

With the abundance of data flowing into or available to the SOC, fusion tools will be required to combine disparate data to form a more complete and coherent picture increasing confidence in critical decisions. Additionally, decision support systems as well as alerting algorithms and mechanisms will need to be developed to extract and highlight the salient information further enhancing the accuracy and speed of security personnel decision making. For example, decision support systems could include the ability to guide personnel through decision trees with a goal of collecting the required information to implement one of several courses of action. Alerting algorithms could issue an audible tone to draw an operator's attention to motion detected at an inappropriate location or at an inappropriate time.

The SOC will also serve as the operational C2 center for all base security personnel as well as the communications center to collaborate with other bases and local authorities. This will require a variety of communications equipment including secure and assured communications channels. The ability to communicate among bases will allow base commanders to level the workload of personnel during times that require surge capability. Thus, if one base is hosting an event, for example Fleet Week, requiring additional security vigilance, another base SOC could receive the appropriate data to help "watch" critical areas. One additional function of the SOC will be to control weapons, both lethal and non-lethal. This will enable personnel to monitor and interdict events at remote locations with reduced manpower resources.

Finally, the ultimate function of the SOC is to create and maintain the COP for base security personnel. Only with situational awareness delivered via the COP within the SOC will the maximum return on security assets be realized.



Technologies for SOC

The SOC will require numerous integrated technologies to achieve full functionality. Many of these technologies are currently available from commercial suppliers. Others are in various stages of readiness. DON resources will be required to leverage commercial technology and development efforts. In fact, strategic investment from a Navy Venture Capital Fund (currently under consideration) could speed time to market for emerging, critical commercial technologies with application to the AT/FP mission.

Example technologies with high impact on SOC operational capability are listed above. At the core of the SOC is the sensor suite supplying data necessary for decision making. Many of the required sensors along with the requisite sensor control and data processing subsystems are currently available from the commercial marketplace. The exception is in the biological sensor area. A fieldable sensor system with the versatility to detect and classify, in real time, the nature of a biological threat is desperately needed. To empower the security force to maximize the potential from the sensor suite, wireless ad hoc communication networks should be employed. This will provide security personnel the flexibility to add or relocate sensors quickly without laying cables or performing cumbersome systems administration tasks.

With the abundance of data available, comes the need for sensor and data fusion tools. All sensing systems, however simple or complex, have a false positive and false negative generation rate. This has major implications on overall effectiveness and information overload. Research advances in automated surveillance including recognition of temporal patterns of activity, anomaly detection, selective attention, and multiple target tracking and forecasting are available in laboratories and could readily be applied to the base security mission. Also of critical importance is the ability to intuitively manage this massive amount of data and information. Commercial technologies in the area of digital multimedia

management systems are applicable. The appropriate data architecture and schema need to be developed and implemented to help insure consistency throughout the Naval Services.

Perhaps the highest impact area for investment of S&T resources is the collection of technologies required to transfer salient, actionable information into the human perception systems for rapid assimilation and decision making. These presentation technologies include visualization systems, audible input and output systems, and tactile feedback systems. For example techniques to visualize multiple sources of information include display metaphors for capturing multiple findings, overlays and registration of information in physical coordinates, and a means for displaying uncertainty and error in situ with information. Decision support systems and alerting algorithms can help focus the attention of the operator, offload workload where appropriate, and augment human cognition where possible. Collaboration tools are essential to enable efficient use of personnel at various Navy and Marine bases as well as interaction with local authorities. These tools will facilitate faster more accurate decision making.

Critical in all SOC operations is the ability to communicate. Lessons learned from the terrorist attacks on the World trade Center and the Pentagon demonstrate the need for interoperable communications. The same need exists in the base security mission. Base security personnel must be able to communicate with local law enforcement and emergency response authorities as well as national level organizations like the FBI and FEMA. Software Defined Radio programs are underway in both the commercial and defense communities. These initiatives must include the communication capabilities of all authorities and organizations impinging on the base security mission. The emergence of third generation (3G) cellular technology and capability in the commercial world will also help empower base security personnel. These capabilities could include wireless internet access and two way image and video transmission enabling broadcast of pertinent information to all security personnel.

Finally, the SOC can have the potential to enable watchstanding personnel to remotely control weapons. These weapons could be lethal or non-lethal. This weapons control application caries with it the ability to reduce security manpower.

Implementation Strategy

- **Lead Base approach**
  - **Risk reduction**
  - **Spiral development**
- **Critical functions**
  - **User/ownership**
  - **Threat vulnerability analysis**
  - **System analysis & integration**
  - **Resource sponsorship**
  - **Acquisition**
- **Reduced manpower funds system acquisition**
  - **Security manpower cost analysis**

Implementation Strategy

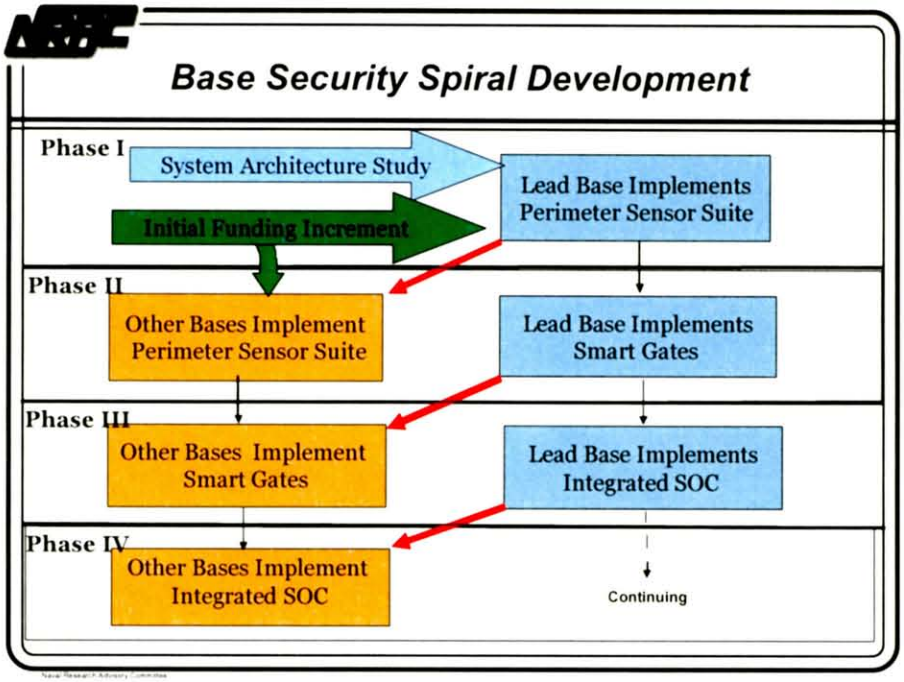
In order to realize the manpower reduction benefits of technology insertion for improved base security with minimal risk and controlled cost, The NRAC study panel envisions a lead base implementation approach. By first developing the necessary overall architecture and then initially installing and operating it piecewise at a single base, the risk and cost associated with multiple, parallel efforts are eliminated. Once each phase of the base security system is proven at the lead base, it will be available for low-risk implementation at other facilities while subsequent phases are being developed and demonstrated at the lead base.

If the lead base approach is to be successful, several critical factors must be addressed. First and foremost, it is crucial that the "owner" of the lead base effort be the ultimate user of the result, i.e. the Fleet Forces Command. Since not all security capabilities will be required or justified for all facilities, threat vulnerability analyses must be performed for each facility to determine what investment is appropriate. It is anticipated that this will be an ongoing process as the threat becomes more sophisticated.

If the optimal balance between capability, cost and manpower reduction is to be achieved, it is essential that the base security enhancement effort be conducted from the top, down. The overall system analysis must be done first to determine the appropriate architecture. The ability to easily and affordably insert new capabilities into the system must be a central part of this effort along with the focus on reducing manpower and making the remaining security force more effective.

It is anticipated that significant savings will accrue from the proposed insertion of technology into the base security effort. However, upfront investment will be required to design the system architecture, implement the lead base and install at least the first phase of

technology before substantial manpower savings are realized. It is therefore necessary that resources be identified and dedicated to this effort in order for it to be successfully implemented and that the acquisition executive is committed to the program. It should be noted that the cost savings realized from manpower reductions might not be directly transferable into security procurement budgets. Therefore, some type of agreement is necessary within the DON that allows for Force reductions cost savings to be used to justify increased security procurement budgets. In order to quantify the likely manpower savings, it is strongly recommended that a security manpower cost analysis be performed as an early part of the effort.



Base Security Spiral Development

The chart above diagrams the phased, lead base approach to implementation of the base security technology previously described. As discussed, the overall base security system architecture must first be designed. Then the first phase of technology will be installed and operated at the lead base. Although it only represents the second largest manpower segment, the panel suggests that installing the suite of perimeter sensors is the best choice for phase one. The risk is low because virtually all the technology is available commercially, the cost is moderate and the disruption to other base functions is minimal. Additionally, this suite of sensors will provide coverage of presently unprotected perimeter areas and will set the stage for automation of base security functions.

Once the perimeter sensor suite is functional, it can be implemented at other facilities while the second phase of technology is being developed and installed at the lead base. Deferring the Smart Gates to the second phase will allow time for the necessary development and integration of the required technologies. By the time Smart Gates are ready for transfer to other bases, manpower savings from the installation of perimeter sensor suites should be available to help defray the costs of installing the gates. As security manpower is eliminated from the gates, savings will accrue very rapidly.

The integration of all base security functions into a SOC will be achieved in phase three. At this point, sensor suites will be installed. Operating and manpower savings from the Smart Gate installations should cover the costs of completing the system. As the threat evolves and security related technologies are continually developed, it is anticipated that the lead base approach will continue to be used to qualify new base security capabilities, but at a lower level of effort than required for the first three phases described here.

This page intentionally left blank

Conclusions

- **Many DoD security efforts ramping up**
  - DoD Physical Security Working Group
  - Joint Service Installation Pilot Program
  - Army & Air Force base security initiatives
  - NASNI AT/FP Technology Test Bed
  - Ongoing base vulnerability analyses
  - North American Maritime Area Surveillance & Tracking (NorMAST)
- **Political issues**
  - Sub-optimal information sharing with other agencies at local level
  - Air perimeter threat
- **Programmatic issues**
  - Bases now proceeding independently
  - Lack of air perimeter defense
  - Application of manpower savings to system acquisition

Naval Research Advisory Committee

Conclusions

Security related efforts are presently receiving broad emphasis within DoD as well as within the commercial and private sectors. In order to reduce the cost of introducing manpower saving technologies into Navy and Marine base security efforts, it is important to track these efforts and incorporate them where appropriate. The DoD Physical Security Working Group is reviewing and testing relevant technologies as is the Joint Service Installation Pilot Program. Army and Air Force bases share similar security problems and the opportunity for joint efforts as well as adopting technologies developed there should not be overlooked.

The Naval Air Station North Island (NASNI) Antiterrorism/Force Protection (AT/FP) Technology Test Bed represents a good approach to vetting technologies for inclusion in the Lead Base security effort proposed in this report. The ongoing base vulnerability analyses conducted by the Naval Criminal Investigative Service (NCIS) are critical to determining what capabilities are needed generally and which should be incorporated into the security programs of specific bases. The U.S. Coast Guard is a valuable ally in monitoring the sea perimeter, and Naval efforts in this regard should be closely coordinated with future Coast Guard efforts like a Maritime Surveillance and Tracking System to achieve early awareness of possible threats within commercial sea traffic.

Some present limitations to establishing the desired levels of base security are not directly addressable by technical solutions alone. Political issues, as well as technical limitations, inhibit real time information sharing among local, regional and national authorities. Although national information sources are always important, especially in early identification of threats, local information sharing can become crucial during developing crises. This can not be accomplished by monthly "coordination meetings" alone, although

such meetings are an important first step. Communication, coordination and information sharing must occur regularly and seamlessly on a day-by-day and hour-by-hour basis. In times of crisis, real time voice and data links are essential in order to maintain situational awareness and develop appropriate responses. Such capabilities can not be established on short notice. It is important to implement regional plans for collaboration with local agencies, but the ultimate success of such collaborations will depend upon the dedicated attention of individual security personnel at each installation.

The air perimeter security problem is largely being ignored at present, being viewed as too hard to handle because there does not seem to be an acceptable technology only solution at present.. However, it represents a major security threat to Naval and Marine bases and therefore to the security of the nation. In addition, it is a common problem for the other services as well as other government installations. Therefore, the DON should take the lead in assembling a group of DoD representatives to establish a formal and official dialog with the Federal Aviation Administration to address the problem. The goal of these discussions should be, at least, the exclusion of VFR flights over bases during elevated FPCONs.

There are also programmatic issues associated with the enhancement of base security through introduction of technology. Bases are now proceeding independently in their attempts to address the security issues discussed in this report. While their initiative is laudable, the result is an inefficient and sub-optimal approach. Resources are being expended to solve the initial parts of the base security problem repeatedly, while little or no attention is being applied to systematic integration of the efforts. Since an integrated security approach will deliver the most effectiveness with the smallest manpower requirement, a top down approach to technology insertion for base security is essential to realizing potential savings.

Although there appears to be the potential for sufficient manpower savings to more than offset the cost of the technology insertion recommended herein, the age-old problem of trading capital investment against reduced operating costs remains. Base security is another area where the total ownership costs of decisions must be carefully weighed. Tight budgets and competition for funds make it easy to defer investment for security related technologies, but the evolving nature of the threat and other more compelling needs for trained military personnel, make the decision particularly critical at this time.

Conclusions (cont'd)

- **Technical issues**
  - COTS elements characterization
  - Recent research advances
    - Recognition of temporal patterns of activity
    - Anomaly detection
    - Selective attention
    - Multiple target tracking and forecasting
    - Advanced biometrics
- **Research issues**
  - Fusing information from heterogeneous sources
  - Multi-source, time-critical decision aids
  - Watchstander effectiveness

Growing awareness of security vulnerabilities in the light of terrorist threats is producing an explosion of security related technologies in all sectors of our society. To avoid inappropriate application of technologies and to insure that the most appropriate components are selected for introduction into the base security environment, some means of accurately characterizing commercial off-the-shelf (COTS) elements is required. The NASNI testbed approach offers an attractive way to qualify candidate technologies for inclusion in the proposed Lead Base security program.

If each security function addressed by technology results in a similar number of personnel watching video or computer monitors, no savings will result. As more and more functions are combined into banks of monitors watched by fewer and fewer people, it becomes difficult to maintain alertness and almost impossible to detect anomalies that may be precursors to crises. It is critical to eliminate the monotony of monitoring routine events and automate the detection of out-of-the-ordinary occurrences. Recent research advances involving establishing daily and hourly patterns of activity, detecting anomalies in those patterns and directing watchstander's attention to such anomalous events, offer effective approaches to dealing with the mass of information collected by the perimeter sensor arrays while substantially reducing manpower requirements. Developments in tracking multiple targets and forecasting likely courses of action could prove invaluable in dealing effectively with evolving situations.

Advances in biometrics are focused primarily in two areas; more reliable identification and remote sensing. Both developments will serve to ease the flow of personnel and traffic at base perimeters while increasing the certainty of correct identification. They will also find application in the tiered security approach to protecting critical assets.

There are also security related issues requiring further research effort. Fortunately many of them are common with the needs of other sectors of society, but DoD and DON specific needs must be addressed by appropriate investment and knowledgeable tracking of other efforts is required if they are to be beneficial to base security efforts. Creating and maintaining a real time COP from such diverse sources as national threat identification reports, perimeter sensor suites and local police and emergency reports requires advances in algorithms to fuse information from heterogeneous sources. Technology to insure time critical decisions are made considering all relevant information from multiple sources is needed and other decision-aide technologies that can improve watchstander effectiveness will insure maximum realization of potential base security manpower reductions.

Recommendation

Implement Technology Based Security System Using Lead Base Program

- Leverage ongoing activities
- Develop advanced security system at Lead Base
- Deploy advanced system at follow bases
- Create IPT to execute program

Naval Research Advisory Committee

Recommendation

The recommendations of the NRAC Technology for Base Security Panel are outlined above. Much of the nation's attention is focused upon homeland security and all such activities have the potential to impact the base security problem. In order to minimize cost to DON, these activities should be followed and their results utilized wherever possible. The Navy and Marine Corps do not have to address security problems alone.

In order to minimize risk and maximize cost savings, a base security architecture should be developed and security technologies should be proven at a lead base before dissemination to other bases. In order to insure the involvement of all parties required for the successful implementation of these recommendations, an Integrated Project Team (IPT) should be assembled.

This page intentionally left blank

Recommendation (Con't)

Technology Based Security System IPT Membership

- **Chair/Owner- CFFC**
- **Resource sponsor - N4**
- **Requirements validation - N34**
- **Acquisition - ASN(RD&A)**
  - **System analyst & integrator - NSWC Dahlgren**
  - **Science & technology - CNR**
    - Automated surveillance
    - Information fusion & visualization
    - SOC human factors
  - **Procurement - COMNAVSEA**

As previously described, the panel considers it imperative that the owner of the technology for base security process be the ultimate user of the resulting product and therefore the CFFC or his designated representative should chair the IPT. It is essential that the resource sponsor, N4, participate in the process and the need for ongoing requirements validation has already been discussed. ASN(RD&A) must be a key participant in the IPT since that office will provide the system analyst and integrator, the S&T investment, and the procurement of the selected technologies, both for the lead base and for the other facilities.

This page intentionally left blank

Appendix A

Terms of Reference
Technology for Base Security
NRAC Summer Study 2002

Objective

Identify technology that can be applied to U.S. Naval and Marine Corps bases to provide the enhanced security for the bases while reducing manpower dedicated solely to security duties.

Background

Immediately following terrorist attacks on September 11, 2001, significant numbers of Navy reservists were reactivated to provide increased security at naval installations. This reaction, along with the use of manpower drawn from the Auxiliary Security Force and close cooperation with local law enforcement entities, was immediate and effective in establishing the safeguards recommended for Force Protection Condition DELTA. CNO subsequently requested a Task Force to:

- Assess the efficient utilization of Naval Reservists in meeting watch standing requirements for FPCON BRAVO and CHARLIE
- Compile and share best practices, lessons learned, and potential uses of technology.

The Task Force concluded that there was technology available that could be applied to both enhance the effectiveness of current efforts as well as improve the efficiency of manpower usage. They also concluded that: "In view of the pace of technology development, a frequent look at the balance between technology and manpower is warranted."

Specific Tasking

Review and assess the application of technology with respect to at least the non-inclusive list of anti-terrorism/force protection (AT/FP) issues: access control, automation, intrusion detection systems, consolidation of manpower, threat detection, counter-surveillance, situational awareness, and deterrence.

Review and assess current research and development of AT/FP technologies and recommend appropriate naval science and technology investment, both near and far term, to enhance base security.

Appendix A

This page intentionally left blank

Appendix B

Briefings and Visits

Commander's Comments	Commander, Fleet Forces Command
Anti-Terrorism/Force Protection (AT/FP)	Commander, U.S. Atlantic Fleet N34
Regional Response/Installation Coordination C2	CO, NAB Little Creek/ Mid-Atlantic Public Safety Program Manager
AT/FP C2 Technical Architecture	Commander, U.S. Atlantic Fleet N617
AT/FP CBRNE	Commander, U.S. Atlantic Fleet N02M2
AT/FP Security	Commander, Naval Region Southeast
Submarine Base, Kings Bay AT/FP Technology Requirements	Commanding Officer, Naval Submarine Base, Kings Bay
Maritime Domain Awareness	United States Coast Guard Marine Safety Office Hampton Roads
AT/FP Naval Station Norfolk	Commanding Officer, Naval Station Norfolk
Naval Surface Warfare Center (NSWC), Dahlgren Division Technology	NSWC, Dahlgren Division
Security Brief	Naval Sea Systems Command
Sandia Special Security Study	Sandia National Laboratories
Rosetel	Angle, Inc.
Force Protection Future Naval Capability	Office of Naval Research (ONR)
N34 Technology	Office of the Chief of Naval Operations (OPNAV) - N34
N34 Flag Comments	OPNAV N34
NSWC Carderock Technology	NSWC Dahlgren Division, Carderock
Threat Brief	Naval Criminal Investigative Service
Bahrain Base Security	ONR
NSWC Crane AT/FP Technology	NSWC Crane Division
Terrorist Mindset	Foreign Service Institute
Naval Undersea Weapons Center, Keyport AT/FP Technology	NUWC Keyport
NSWC Coastal Systems Station (CSS), Panama City AT/FP Technology	NSWC Panama City, CSS

Appendix B

Common Access Card Report	NRAC
Update on Subcutaneous chips	NRAC
Portable Vehicle Arresting Barrier	General Dynamics
DOE Security Programs	Department of Energy
Active Denial Systems	Raytheon
USMC Programs	Marine Corps Warfighting Laboratory
National Incident Control and Action Communication System (NICACS)	Federal Marketing Alliance, Inc.
Visits	
Naval Criminal Investigative Service	Washington, DC
Naval District Washington Headquarters	Washington, DC
Federal Bureau of Investigation	Clarksburg, WV
National Institute for Occupational Safety and Health	Morgantown, WV
Department of Defense Common Access Card Program Management Office	Arlington, VA
U. S. Navy Common Access Card Program Management Office	Mechanicsburg, PA
Naval Region Southwest	San Diego, CA
NAS North Island Operations Department	Coronado, CA
SPAWAR Systems Center	San Diego, CA
Telephone Discussion	
Food and Drug Administration	

Appendix C

CAC CARDS AND BIOMETRICS

Common Access Card (CAC)

- **Background Information**
  - DoD Standard Smart Card currently available (with scheduled enhancements).
  - Navy has no standard access control card
  - Each DoD CAC is registered to user with fingerprint and pin information
- **Card Features**
  - Printed Information - picture/ name/ rank/grade/issue and expiration
  - Semiconductor RAM - PKI public/private keys-X509 Certificate, PIN, fingerprint, and biometrics
  - Magnetic Stripe - SEIWG 012 credential number
  - Bar Codes (1D and 2D) - Available for Local Applications
  - Biometrics - to be added in 5/03; options being studied by DOD Biometrics Management Office
  - Potential New Feature - retro-reflective (IR) ink for "fast pass" imaging
- **Proposed Usage**
  - Gate Entrances, Building Access, Network and IS, Timed-Access Control Areas, Visitor, Contractor and Supplier ID, Visit Requests & Clearance processing
- **Recommendations**
  - Navy needs to adapt DOD CAC standard
  - Navy should add Retro-reflective (IR) ink for identification

Naval Research Advisory Committee

Common Access Card

The Common Access Card is DoD's standard smart card identification technology. Over 750,000 CACs have been issued. The card is used as a source of identification, access control, and individual information for uniformed active-military personnel, dependents, DoD civilian employees, selected reserves and eligible contractors. CAC's are registered via remote registration through the RAPIDS (Random Access Personnel Information Dissemination System) workstations. Fingerprint information is recorded at the time of registration, but this information currently is only used for identification purposes when the card needs to be modified or replaced. All card registration information is tied to the Defense Enrolment Eligibility Reporting System (DEERS).

Each card costs approximately $5 and the cost is expected to move down to $1 in higher volumes. Since there is no standard access control system in the Navy, the CAC offers an existing, cost-effective, and efficient infrastructure for achieving standard access controls.

The DoD CAC accommodates several forms of data storage. The first of these is printed information, which includes picture, name, rank, grade and issue and expiration dates. It also incorporates a tamper-proof RAM and integrated circuit processor for storing and processing PKI public/private encryption keys and X509 certificates and other application related data. Magnetic stripe technology is used for storing SEIWG 012 credential numbering descriptors, and both one-dimensional and two-dimensional bar codes are incorporated for local applications. In addition to these features, the DoD CAC office plans to add improvements and enhancements as technologies mature, specifically biometrics. The DoD Biometrics Management Office will play an important role in

determining the specific biometrics that will be incorporated on the card. The first set of CAC biometrics capabilities to be deployed will be fingerprint biometrics, scheduled to be introduced by May of 2003. Retro-reflective IR bar codes, which can be imprinted on the back of the card, are also being considered. These would allow reading identification codes at low speeds and at distances of several yards.

Currently, the cards require physical contact with readers. The second generation of cards, scheduled for late Fall of 2002, will allow for a radio frequency (RF) proximity link that enables information to be transferred without contact. The entry of additional information, such as PIN or biometric data, will still require contact; however, such data may only be required under higher security/threat conditions.

The CAC can be used for access control to gate entrances, buildings, restricted areas, networks and information systems. Furthermore, CAC compliant smart cards can also be issued locally and be used for controlling visitors, contractors, and suppliers. The card can be used as a secure method of processing clearances and allowing temporary (timed) access to the base and certain restricted areas.

Biometrics

- **Current technologies**
  - Iris / retinal scanning
  - Thumbprint recognition
  - Face recognition
  - Subdermal RF microchip
    - Acceptance issues, perhaps employ selectively for only for most secure areas
- **Emerging & future technologies**
  - Enhanced recognition (face, iris, etc.)
    - Image processing for greater distance and accuracy
  - New modalities
    - Rapid PCR for DNA forensics
  - Multimodal biometrics: combinations of modalities in sequence or parallel to increase reliability
    - *e.g.*, voice + face analysis, thumb + face, etc.
- **Recommendations**
  - Value of high-throughput biometrics at perimeter
  - Tiered designs based on throughput vs. accuracy tradeoff
    - Can tolerate slower, more accurate biometric recognition for sensitive areas
  - Fast-paced commercial development makes special Navy investment irrelevant, redundant

Naval Research Advisory Committee

Biometrics

Applied methods utilizing biometrics currently deployed in various civilian and military settings include iris and retinal scanning, and thumb and face recognition techniques. Subdermal RF microchips have been used for some years in animals, most notably in dogs with registry with the American Kennel Association. This technology is increasingly advocated for use in humans and has in fact been utilized in several anecdotal situations. There seems to be considerable resistance in the private sector to this approach, in some cases on religious grounds. The Food and Drug Administration (FDA) has as of this time not made a final determination whether they will regulate these devices when medical information is not encoded on the microchips. There are no known or anticipated biological hazards associated with their implantation. Their use might be considered in specialized circumstances involving critical personnel in sensitive jobs.

Emerging and future technologies include enhanced face and iris recognition as a result of next generation image processing for greater distance and accuracy. Also on the horizon is the ability to apply high speed polymerase chain reaction (PCR) for deoxyribonucleic acid (DNA) analysis. This technology, too expensive for general use, may be applied in special circumstances requiring highly accurate identification. For more general application multimodal modalities in sequence or parallel will increase reliability exponentially, e.g. voice plus face analysis, thumb plus face, etc.

This page intentionally left blank

Appendix D

ACRONYMS

3G	Third Generation
ASN(RDA)	Assistant Secretary of the Navy (Research, Development & Acquisition)
AT/PF	Antiterrorism/Force Protection
ATM	Automated Teller Machine
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Common Access Card
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
C4I	Command, Control, Communications, Computers and Intelligence
CFFC	Commander Fleet Forces Command
CNO	Chief of Naval Operations
CONOPS	Concept of Operations
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf
DEERS	Defense Enrollment Eligibility Reporting System
DNA	Deoxyribonucleic Acid
DOD	Department of Defense
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPCON	Force Protection Condition
IPT	Integration Process Team
IR	Infrared
NASNI	Naval Air Station North Island
NCIS	Naval Criminal Investigation Service
NRAC	Naval Research Advisory Committee
OPNAVINST	Office of the Chief of Naval Operations Instruction
PCR	Polymerase Chain Reaction
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RAM	Radar Access Memory
RAPIDS	Random Access Personnel Information Dissemination System
S&T	Science and Technology
SEIWG	Security Enterprise Integration Working Group
SOC	Security Operations Center
SSN	Social Security Number
TF	Task Force
TOR	Terms of Reference
UCAV	Unmanned Combat Air Vehicle
UGV	Unmanned Ground Vehicle
VFR	Visual Flight Rules

This page intentionally left blank