AU/ACSC/143/2000-03

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

OPTIMIZING COMPUTER NETWORK DEFENSE TRAINING

by

Todd M. Piergrossi, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Joel Junker

Maxwell Air Force Base, Alabama

April 2000

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-04-2000	Thesis	xx-xx-2000 to xx-xx-2000

4. TITLE AND SUBTITLE
Optimizing Computer Network Defense Training
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Piergrossi, Todd M. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Air Command and Staff College
Maxwell AFB, AL36112

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Computer Network Defense (CND) is inseparable from the daily responsibilities of the communications professional: establishing, operating, and optimizing the voice, video, and data network. The Tactics, Techniques and Procedures (TTPs) involved in responding to a Computer Network Attack (CNA) incorporate the identical tools used by the Network Control Center (NCC) when operating the network. In essence, CND is a subset of Information Assurance. In order to thwart the emerging Information Warfare threat, the Air Force needs to recognize and capitalize upon the similarities between CND and daily Information Assurance tasks. The critical linkage necessary to codify CND functionality is training. Commercial industry, as well as a number of uncoordinated military initiatives, has developed an extensive CND toolkit. Despite these technological innovations, current CND training as practiced by the USAF, suffers from inappropriate requirements development and a lack of disciplined synchronization with training opportunities. This paper will present the sources of CND training requirements, summarize the CND training opportunities currently available, and then suggest a promising Human Resource Management (HRM) methodology for linkage and synergy.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	47	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

Disclaimer

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

Contents

Page

List of Tables

Page

Preface

Too often in the communications career field we get caught-up with the issues surrounding technological capability and software gimmicks, at the expense of the mission. We become servants of "the box", always seeking to increase computing or memory capacity without fully acknowledging the underlying principles that actually make or break the mission. Arguably, the single most critical factor that communications leadership can influence to ensure mission objectives are obtained is the development of a skilled workforce ... the people are and always have been the fundamental communications enabler.

This analysis seeks to rekindle the initiatives that focus the Information Assurance mission back onto its most fundamental building block and valuable resource; training the kids in the trenches so they can effectively perform their jobs. I hope this analysis will provide one possible direction to standardize Computer Network Defense (CND) training; thus eliminating the ad hoc and "county option" methods currently employed by supervisors in developing their training plans.

Finally, I'd like to acknowledge the efforts of Major Von Gardiner, for partnering with me in thinking through the Information Assurance construct. His unique insight into how operations should be conducted in order to deliver Information Superiority to the warfighter provided tremendous dividends towards the completion of this analysis.

Abstract

Computer Network Defense (CND) is inseparable from the daily responsibilities of the communications professional: establishing, operating, and optimizing the voice, video, and data network. The Tactics, Techniques and Procedures (TTPs) involved in responding to a Computer Network Attack (CNA) incorporate the identical tools used by the Network Control Center (NCC) when operating the network. In essence, CND is a subset of Information Assurance. In order to thwart the emerging Information Warfare threat, the Air Force needs to recognize and capitalize upon the similarities between CND and daily Information Assurance tasks. The critical linkage necessary to codify CND functionality is training. Commercial industry, as well as a number of uncoordinated military initiatives, has developed an extensive CND toolkit. Despite these technological innovations, current CND training as practiced by the USAF, suffers from inappropriate requirements development and a lack of disciplined synchronization with training opportunities. This paper will present the sources of CND training requirements, summarize the CND training opportunities currently available, and then suggest a promising Human Resource Management (HRM) methodology for linkage and synergy.

Part 1

Introduction

Computer Network Defense (CND) is a recently identified subset of the United States Air Force's (USAF) Information Operations doctrine, falling under the auspices of Information Assurance. Because it is such a new field of operations, personnel expertise, operational planning, and employment is greatly lagging behind the potential of technical capabilities. Additionally, the knowledge, skills, and abilities (KSA) associated with CND operations are inseparable from the KSAs required by the communications professionals for operating, maintaining, and optimizing the voice, video, and data networks that transport our most vital warfighting data and information.[1] The tactics, techniques, and procedures (TTPs) involved in responding to a Computer Network Attack (CNA) incorporate the identical KSAs and tools used by a Network Control Center (NCC) or Network Operations and Security Center (NOSC) when operating on a daily basis. In order to thwart the emerging Information Warfare threat, the USAF needs to recognize and capitalize upon the similarities between CND requirements and Information Assurance requirements. This linkage and subsequent training methodology has not yet been correctly established.

Until the USAF identifies a workable training solution to field the necessary CND operators, numerous ramifications could present themselves: a) USAF networks will be vulnerable to even the most elementary CNAs, thereby denying commanders the information necessary to prosecute

aerospace operations; b) Commanders will perceive CND training as having little potential for return on investment (ROI) and therefore not place their limited financial and personnel resources into the CND training cycles; c) Personnel will be assigned to CND duties and perform them in an ad-hoc manner, creating seams of vulnerability for a potential adversary to penetrate; d) Untrained and unqualified personnel will attempt to execute CND courses of action and mistakenly commit information fratricide. All of these consequences negatively impact USAF operations and create an increased potential for both mission failure and loss of life.[2] The issue of concern is whether the USAF can optimize its current CND operations, specifically in the area of training, by capitalizing on synergies realized between established Human Resource Management (HRM) practices and Information Assurance toolkits and TTPs.

Currently, CND operations within the USAF do not use a validated (i.e., recognized within the HRM profession of study) process to develop training requirements. Instead, local training managers and supervisors employ any number of impromptu techniques to derive unique and unsubstantiated training requirements. Additionally, the synchronization of these unsubstantiated training requirements to the myriad of CND training opportunities is conducted in an ad hoc fashion. This unstructured training methodology severely degrades the USAF's CND capabilities. Today's CND training is focused on a point-defense functionality, deficient of the integrated, network centric approach necessary to execute the seamless courses of action (COA) required to defeat even the simplest computer network attack (CNA).

This research paper identifies CND training deficiencies by examining the sources and methods of the current CND requirements development process. It also examines methods employed to synchronize CND requirements-opportunity training. Section three introduces a validated[3] HRM process as a mechanism to accurately derive CND training requirements as a

solution to the CND training dilemma. This HRM process, referred to as a skills-based analysis, produces the information pertaining to qualification and job content so training programs can be tailored to the unique nature and characteristics of the work.[4] These substantiated requirements are then married to available training opportunities using a structured synchronization template. The final product is a cost effective CND training program that capitalizes on the Information Assurance capabilities currently available.

Because CND training methodologies have not yet proven themselves in terms of cost, time, and mission effectiveness, command authorities will continue to view this critical mission enabler as one of only limited importance. As such, CND training will not receive the leadership emphasis and resource allocation necessary to ensure this portion of the USAF's Information Superiority core competency.

Notes

[1] United States Air Force Concept of Operations, *Concept of Operations for the Network Operations and Control Center*, 14 January 1999, 5.

[2] Air Combat Command Manual, *Tactics, Techniques and Procedures for the Operation of the Network Weapon System*, October 1999, 2.

[3] George T. Milkovich, *Human Resource Management* (Chicago: McGraw-Hill, 1997), 79.

[4] Ibid., 84.

Part 2

CND Operations Requirements

Requirement sources governing military CND operations can be divided into three categories: military doctrinal documents, commercial industry sources, and ad hoc sources. These governing materials provide standardized strategic-level, standardized tactical-level, and non-standardized tactical-level guidance pertinent to conducting CND operations. Doctrinal documents present fundamental principles that guide the employment of forces, offering a common perspective from which to plan and operate. These documents fundamentally shape the way leaders plan and train for war.[1] Commercial industry sources, which are typically underwritten by network vendors, provide exceptional detail into the highly technical, tactical-level CND tasks and skills required for the performance of those tasks. Ad hoc requirements are those low echelon, i.e., squadron-level, demands that identify and resolve tactical-level dilemmas independent from the concept of an integrated, interdependent network centric environment.

Doctrinal Guidance

Joint Doctrine

Joint doctrine governing Information Warfare (IW), Joint Pub 3-13, was approved by the Chairman, Joint Chiefs of Staff, in October 1998. It presents the fundamental principles that guide the employment of IW forces throughout the full spectrum of operations: peace,

competition, crisis, and conflict. Joint Pub 3-13 is the keystone document for CND operations. It establishes the foundation for all CND strategies, objectives, COAs, and tasks. Because this is a strategic-level document of the highest order, it is restricted to defining the fundamental principles and how those principles integrate into a cohesive capability for the Joint Force Commander. Any relationship from Joint Pub 3-13 to requirements for CND operations is either developed through a series of supporting documents that relate down to the tactical-level, or the relationship has been inappropriately extrapolated based on assumption.

Air Force Doctrine

Air Force doctrine governing Information Warfare (AFDD 2-5) was approved by the Chief of Staff in May 1999. Additionally, the USAF Concept of Operations (CONOPS) for Information Operations was approved in December 1999. These documents use the guidance provided in Joint Doctrine Pub 3-13 to codify the Air Force vision for integrating and conducting information warfare through the full spectrum of operations; establishing the basic parameters for organizing, operating, and employing Air Force assets to obtain information superiority. Within AFDD 2-5, the Information Assurance mission and its CND subset are addressed. Both sources also include generalized instructions for IW education and training, directing the implementation of four initiatives pertinent to CND. First, the CONOPS specifies the development of an Information Warfare Applications Course (IWAC), intended to educate mid-level IW operators in the application of IW doctrine and principles. IWAC provides a forum for discussion of the capabilities and vulnerabilities of IW at the operational and tactical-levels of war. Second, AFDD 2-5 delegates responsibility for specific training requirements development and implementation to the Career Field Manager for each Air Force Specialty Code, i.e., Specialty training. Third, both sources present a requirement for ancillary training to update

IW/CND operators on the most current changes in IW; exposing them to the newest threats and technologies. Finally, the CONOPS directs the development of mission specific training for IW/CND operators to obtain and maintain a mission certification status. Identification of specific job tasks, systems components, knowledge, skills, and abilities (KSAs) or training methodologies are not included in either document

Air Force Tactics, Techniques and Procedures (TTPs)

KSAs pertaining to military CND operations are only partially developed in the Air Force's Tactics, Techniques, and Procedures (TTPs) manuals. TTPs establish a standardized tactical-level framework for the operation of a weapons system; specifying standard formations, tactics, command and control (C2) procedures, and the like[2]. *Tactics, Techniques and Procedures for the Operation of the Network Weapon System* is the sole military document codifying tactical-level CND operations. It was developed and formatted with respect to the Air Force's "3-1" series of manuals, which specify the TTPs for every flying weapons system in the inventory. This document identifies the crew positions, crew responsibilities and how these positions are integrated into a synergistic defensive capability for both the tactical-level Network Control Center (NCC) and the operational-level Network Operations and Security Center (NOSC). Additionally, it presents the C2 mechanisms, rules of engagement, and standard systems configurations necessary to ensure information superiority. More significantly however, this TTP manual defines the differences between passive and active CND operations (Table 1) and also specifies the matrix of available CND countermeasures tactics (Tables 2 and 3) available to operators to thwart computer network attacks (CNAs).[3]

Table 1. Passive and Active CND Definitions

Passive Network Defenses are the basic evasive maneuvers for the network weapon system. Network Defense is the strategy of proactively implementing security countermeasures and policies to eliminate vulnerabilities and/or robust the defensive posture of all enterprise sensors, services, applications, and customers. The goal is to secure the blue network order of battle and required information flow. Formations for establishing the standard network defense posture are described in Chapter Two. Network Defense Controllers utilize these countermeasure capabilities.
Active Network Defenses are analogous to Advanced Combat Maneuvers for network weapon system defense. The NOSC and/or the NCC reactively execute tactics, techniques, and procedures in direct response to hostile, malicious, or unintended network intrusions and IAW established ROE. Active Network Defense seeks to maintain operational availability of the blue network in sufficient capacity to meet required information flow.

Table 2. Passive Network Defense Countermeasures

COUNTERMEASURE	PURPOSE
Access control	Provides filters and rules for allowing or blocking entry
Authentication controls	Establish mechanism to determine the identity of a user or device
Encryption	Conversion of data to undecipherable form for secure transmission and decryption at destination
External Router	Provides pre-determined filtering and blocking capability (and the installation service delivery point)
Firewall	Provides a barrier to intruders at a selected boundary
Hardened OS	Proxy or other server that is robust enough to resist malicious activity or intrusion
Intrusion detection	To detect unauthorized access to militarily sensitive data
Operational Risk Management	Manage Enterprise-wide risk mitigation through positive control of passive network defense security measures
Passwords	To authenticate identity or authorize access to data
Software patch	To fix specific computer software problems
Proxy	Determines user or client IP authorization for further connection to a remote destination

Table 3. Active Network Defense Tactics

TACTIC	PURPOSE
Detect	Establish awareness of unauthorized network activity/intruder to support defense of resources
Isolate	Segregate suspected activity/intruder from authorized users to contain and limit access
Monitor	Watch intruder to determine purpose or operating procedures
Redirect/Control	Control activity/intruder and destination
Terminate	End intruder session in order to deny network access
Reinforce	Reinforce is a brute force tactic used to overcome a network assault by applying excess capacity to initiate backup and repair inside the intruder's damage cycle.
Evade	Evade is used to avoid the enemy's attempt to engage or monitor.

Although the TTP document for the network weapon system provides the information necessary to initiate and operate a CND mission, it lacks any specifications for CND mission training. Specifically, the TTPs are deficient in identifying both the KSAs required to perform the work (e.g., software scripting, network traffic analysis, and network mapping) and the job tasks that are incorporated within the work (e.g., programming a firewall, configuring a router, and controlling network addressing). The TTPs address how the CND mission should function but it does not identify precisely what the work of the CND operators entails. This limitation is attributable to the immaturity of both the concept of CND operations and the initiative to codify CND operations within a TTP manual. The entire area of study is too new; all the particulars have not yet been adequately identified and resolved.

Commercial Industry Sources

Commercial industry sources that identify CND requirements include a diverse realm of "hacker" textbooks, technical whitepapers from both academia and vendors, and private business network operation centers. The principle orientation of these sources is passive CND; proactively implementing security countermeasures and policies to eliminate vulnerabilities and robust the network's defensive posture. Passive CND maintains a direct analogy to those measures employed by combat units in their force protection efforts; including the hardening of structures, identification checkpoints, camouflage, and stealth.

Textbooks

A review of the top-five selling computer hacker textbooks[4] found no reference to CND training methodology. Instead, all the textbooks followed a similar format for presenting its materials: examination of the atypical threats, vulnerability analysis of the most commonly implemented network services, identification of point-defense capabilities, and a review of operating procedures for those point-defense toolkits. In essence, these texts provided an extensive shopping list of Information Assurance tools and a brief (a.k.a. superficial) step-by-step review of how to operate them. Currently, there are over 1500 officially recognized CNA threats documented by Carnegie Mellon University.[5] These threats are categorized into seven generic attack methodologies shown in Table 4.[6] None of the top-five selling computer hacker textbooks correlated potential threats against available countermeasures, nor did they attempt to sequence the countermeasures into an active CND course of action.

Table 4. Generic Attack Methodologies

TYPES of ATTACKS	EXPLAINATION
Masquerade/Spoof	Pretending to be a different entity: user, process, or node
Social Engineering	Bypassing security measures by exploiting human factors
Replay	Repeating part of a message to produce unauthorized effects
Denial of Service	Disabling access to or availability of network services
Trojan Horse/Virus	Authorized function that hides an embedded unauthorized function
Data Theft	Wiretapping that allows stealing and interpretation of private data
Data Corruption	Partial or total loss of data integrity

Whitepapers

Technical whitepapers are primarily underwritten by vendors and thus maintain an inherent bias towards those particular products and/or services that complement their markets. Even research conducted by academia was typically affiliated with some private business sponsorship that must be understood for potential influences towards certain preordained conclusions or recommendations. In this light, technical whitepapers present no added value when trying to derive specific CND training requirements.

However, whitepapers are extremely useful in understanding the detailed workings of a vendor's product line, and the underlying implications of proposed courses of action. Additionally, whitepapers can supplement the development of operational concepts that are superficially presented in textbooks. More specifically, the correlation of whitepaper data presents the CNA threat as one that: maintains multiple threat axis (i.e., attacks through the primary Internet connection, an unsecured backdoor modem, or an internally injected virus); utilizes deception, faints, and decoys; takes advantage of temporal dimensions (i.e., a slowly

timed attack with small pieces of the attack tools penetrating the network over a course of days, vice milliseconds); and may only be detected as a performance anomaly.[7]

Network Operation Centers

Private commercial businesses provide CND functionality through either inherent or outsourced Network Operation Centers (NOCs). These NOCs would be equivalent to the Air Force's NCCs and/or NOSCs, depending on if they were functioning at the tactical or operational levels. They all maintained some form of "crew position" concept of organization for task management purposes, generically presented in Table 5.

Table 5. Commercial NOC Crew Positions

CREW POSITION	JOB DESCRIPTION
Crew Commander	Responsible for crew operations and overall Information Assurance
Infrastructure Control	Responsible for optimized performance of network architecture
Applications Control	Responsible for optimized performance of network services
Data Flow Control	Responsible for optimized flow of mission critical data
Network Defense	Responsible for all aspects of security: active and passive CND
Customer Support Interface	Single point of contact for resolving customer requirements

Commercial NOCs such as those at AT&T, Ford Motor Company, Hyatt Hotels, Federal Express, or HUMANA Medical maintain a high degree of security surrounding their CND methodology. They do this to reduce the ability of a potential threat to conduct intelligence preparation of their battlespace (IPB) and also to protect proprietary passive CND capabilities (i.e., software programs, infrastructure architectures, and C2 processes). Although the details of their operations cannot be released, their general approach to CND is via passive CND

mechanisms, designed around a point-defense methodology (Table 6).[8] That is, each networked device is considered autonomous and configured with the basic array of security capabilities. Their simplified process is:

1. Detect and eliminate vulnerabilities
2. Employ countermeasures on a point-defense schema
3. Implement an intrusion detection system
4. Establish rigorous post-attack reconstitution and recovery procedures

Table 6. Commercial NOC CND Training Requirements

REQUIREMENT	PURPOSE
Access control solutions	Provides filters and rules for allowing or blocking entry
Authentication controls solutions	Establish mechanism to determine the identity of a user or device
Encryption solutions	Conversion of data to undecipherable form for secure transmission and decryption at destination
Router configuration	Provides pre-determined filtering and blocking capability (and the installation service delivery point)
Firewall configuration	Provides a barrier to intruders at a selected boundary
Operating System configuration	Proxy or other server that is robust enough to resist malicious activity or intrusion
Intrusion detection	To detect unauthorized access to militarily sensitive data
Vulnerability detection	To fix specific computer software problems
Program scripting	Create special purpose, just-in-time software to capture and analyze data

Ad Hoc Demands

Ad hoc demands are those security initiatives that pop-up independent of a synergistic, integrated CND strategy. It is point-defense taken to the extreme. Theses ad hoc requirements are typically a knee jerk reaction to the combined affects of marketing propaganda, leadership naivete, poor network engineering discipline, and political posturing for allocation of funding. An example of ad hoc requirements was the October 1998 emphasis on Firewall technology and technician KSA development. During this period, firewalls were intensely marketed by

commercial vendors as the Holy Grail of CND security. Base-level emphasis on implementing firewall technology accelerated due to the realization that mission critical networks were poorly engineered to defend against certain, vendor-marketed types of threats. Independently, USAF bases began installing firewalls and requiring certified IW operators to maintain these devises. The final result was a heterogeneous application of technology and CND capabilities that neither improved the security of the networks nor reduced the total cost of ownership. In the end, ad hoc demands created a "Maginot Line" network defense that was easily bypassed by adversaries and squandered precious manpower, funding, and time resources. The myriad of ad hoc demands currently requires over 200 training days for the average technician to fulfill[9]. Although ad hoc demands should not be considered the primary source for developing CND training requirements, there is some value achieved by including them into a disciplined, work analysis process. If used correctly, ad hoc requirements can be a benefit to the overall success of the CND mission; if abused they become a significant detractor.

Notes

[1] Joint Doctrine Publication, *Joint Doctrine Capstone and Keystone Primer*, 15 July 1997, 2.

[2] Air Combat Command Manual, *Tactics, Techniques and Procedures for the Operation of the Network Weapon System*, October 1999, vii.

[3] Ibid., 39-52.

[4] *The Security Store@Infowar.com*, Infowar, 1999, n.p.; on-line, Internet, 3 December 1999.

[5] Carnegie Mellon, *Alert Statistics*, 1999, n.p.; on-line, Internet, 10 December 1999.

[6] Uday O. Pabrai, *Webmaster Administration Certification Exam Guide* (New York, McGraw-Hill, 1998), 116.

[7] John D. Howard, *An Analysis of Security Incidents on the Internet*, 2 April 1997, n.p.; on-line, Internet, 10 December 1999, www.cert.org/research/JHThesis/chapter6.html.

[8] Internet Engineering Task Force, *Site Security Handbook – RFC 1244*, July 1991, n.p.; on-line, Internet, 12 November 1999, ww.alw.nih.gov/Security/FIRST/papers/general/handbook.txt.

[9] Air Force Communications Agency, *Network Management Training Tracks*, 22 April 1998, n.p.; on-line, Internet, 17 November 1999, wwwafca.scott.af.mil/gc/gcl/optn/operate/rules/33115v2.htm.

Part 3

Analysis of CND Operational Training

Similar to the CND requirements presentation, CND operational training can be divided into three categories: codified military processes, commercially available opportunities, and ad hoc military initiatives.

Codified Military Processes

Codified military CND training is being tackled from two fronts: the Information Operations arena sponsored by the Operations/Intelligence communities and the Information Assurance arena sponsored by the communications community.[1] This dual training responsibility is directly attributable to the ambiguities written into both AFDD 2-5 and the USAF CONOPS for Information Operations. Despite this atmosphere of competition and redundancy, significant strides have been made over the past three years to develop both operationally and cost effective training opportunities. One area where the military is deficient is aggressor training; a different approach from the popular Intelligence Aggressor Support Teams. While the Aggressor Support Teams attempt to attack and defeat a friendly network and then provide "lessons learned", aggressor training institutionalizes an adversary's mindset and operational techniques into the CND operator's intuitive reactions. Systematic military CND training includes the following:

Information Warfare Applications Course (IWAC).

IWAC is sponsored by the Operations community and is intended to educate mid-level IW operators in the application of IW doctrine and principles. It provides a forum for discussion of the capabilities and vulnerabilities of IW at the operational and tactical-levels of war. Course of action (COA) sequencing is not addressed at present but may be addressed in this course at a future date.[2] The big drawback is that this course provides no specific, hands-on technical skills development. Consequently, it can not be considered as a viable training opportunity to fulfill CND operational training requirements.

Base Information Protection (BIP) Equipment Suite Training.

BIP training is sponsored by the communications community. It consists of 7 weeks of training at a military facility. Re-packaged product vendor materials are used for each point defense product. Training consists of CND toolkit installation, operation, and maintenance. Course of action (COA) sequencing and the integration of point-defenses into a systematic, defense-in-depth capability are not addressed in this training opportunity.[3] The primary reason for this operational deficiency is that the USAF closely followed the vendor's marketing strategy during its re-packaging efforts in order to rapidly field some form of CND capability, regardless of how remedial its functionality. The vendor's marketing approach targets a quick fix, low cost defensive solution. The Air Force mimicked this approach for BIP training, failing to explore the synergies available through product integration.

Automated Security Incident Measurement (ASIM) Training.

ASIM training is sponsored by the Intelligence community. It consists of 7-10 days of training at a military facility. Students get hands-on instruction for the installation, operation, and maintenance of a singular intrusion detection and point defense product. CND tactics

training is limited to *Detect* and *Terminate* (IAW Table 1: CND Tactics). Only one technique is utilized under the *Terminate* tactic; blocking the offending IP address. This approach is singular in nature and ineffective if employed in isolation of other tactics. An adversary can easily defeat this defensive strategy by attacking from multiple originating network addresses; dispersing the apparent source of the attack. Such was the case during the February 2000 denial-of-service attack against high profile e-commerce and Internet companies.[4]

Information Protection (IP) Operations Certification.

IP certification is sponsored by the Communications community. It consists of 11 weeks of scripted Computer Based Training (CBT) in conjunction with 18 weeks of classroom and hands-on instruction. IP certification provides detailed training in 120 subject matter areas, all based on an independent, point defense philosophy.[5] Technologies are not integrated to provide a comprehensive, defense-in-depth functionality. Additionally, no course of action (COA) sequencing is presented. This course retains significant value to CND operations if it is properly synchronized against valid CND training requirements. However, as a stand-alone training process it is overwhelming in both scope and complexity, providing limited utility to the CND mission.

Commercially Available Opportunities

Commercially available CND training opportunities encompass the entire cost versus capability spectrum as depicted in Table 7.[6] Any consideration for their potential utilization must account for cost v. capability differentials in order to achieve the greatest possible business efficiencies; remembering that financial resources are currently constrained in the military.

Table 7. Cost Vs. Capability Matrix for Commercially Available CND Training

Simulators Low Cost – High Capability	Consultant Aggressor Training High Cost – High Capability
Vendor Product Training Low Cost – Low Capability	Consultant Prevention & Recovery Training High Cost – Low Capability

The majority of commercially available training opportunities revolve around vendor point-defense product lines and are vendor sponsored; hence they should be considered biased until proven otherwise. Consultants and third party integrators typically offer more of an integrated systems approach rather than a point-defense approach, resulting in a better cost per capability efficiency rate. Utilizing commercially available training opportunities removes from the military the cost burdens associated with maintaining a comprehensive training core competency subject to rapidly evolving technology and techniques. Additionally, this method of training capitalizes on the extensive pool of both manpower and expertise available to the private sector.[7] Projecting the burdens of maintaining technical expertise and manpower capacity to the commercial sector affords the military significant flexibility in addressing the myriad of CNA and abating the most serious threats in a timely manner. Commercially available CND training can be categorized into the following four methodologies:

Vendor Sponsored Product Training.

Each toolkit/product is presented and trained as an isolated, independent entity. Training can typically be provided either at the customer's site or at the vendor's facilities. A review of several vendor offerings reveals that costs range anywhere from $500 per day to $5000 per week,

per trainee. Training provided by the vendor at the customer's facilities normally reduces overall training costs by 50-75 percent, depending on location and number of students in attendance. Vendor training is available for all point-defense products currently under acquisition or implemented in the USAF Information Assurance and Information Warfare programs.

Consultant Sponsored Prevention and Recovery Training.

This methodology provides a more robust systems-integrated approach. Vulnerability analysis training is performed across multi-vendor and heterogeneous infrastructures and application suites, using a variety of point defense toolkits. Risk abatement processes are taught using any number of vendor products and technique sequences. Within this methodology the bottomline line is that there is no one specific technique or product to protect against a CNA. The student must have a working knowledge of network principles and services in order to successfully complete this type of training. Again, location options are available, either on-site to provide tailored customer training or at the consultant's facility to acquire generic expertise. A course abstract of a typical consultant sponsored training opportunity is as follows:

> Intrusion Detection & Analysis Course: Explore a wide variety of tools and techniques to detect and respond to vulnerabilities, external attacks, and internal policy violations. Detect common attack signatures as well as analyze system and network logs to identify new vulnerabilities and attacks.[8]

Consultant Sponsored Aggressor Training.

This methodology affords the CND operator the opportunity to master their KSAs by exercising integrated COAs in a "live fire" environment. Consultant teams normally execute a series of attacks against the network, simulating the indications and effects of an actual CNA. The focus of this training opportunity is not identification of remedial CND tasks, but rather the further development of advanced skill sets. Consultant sponsored aggressor training should only

be employed once a sound foundation of basic CND skills has been developed. Financial costs for this methodology are in the higher end of the spectrum due to the requirements for use of a consultant attack team, time needed to conduct pre-attack reconnaissance, duration of attack, analysis of results, and finally debriefing and knowledge transfer. A typical course abstract is as follows:

> Attack & Defend Course: Explores the risks of Internet connectivity using the latest hacker tools and techniques and through an in-depth examination of the vulnerabilities in TCP/IP network protocols, focusing on common threats to the confidentiality, integrity, authenticity, and availability of networked resources. Provides customers with the knowledge and skills necessary to identify and prevent the majority of network attacks using multi-vendor network security tools.[9]

Simulator Training.

A recent innovation in the area of CND training is the advent of CND simulators. These training tools are akin to common "flight simulators" used by Air Force pilots, only their mission is secure computer and network operations management. The CND simulator provides a semi-controlled experience in which to exercise varied proactive defensive measures, practice detection and mitigation of malicious incidents, and to effect proper reporting of significant security events. The central objective of the simulator training scenarios is to find and exercise the "best path" as the student balances two competing needs.[10] The student is charged with the responsibility of maintaining a system or network. They need to keep this system active and available in order to support the greatest number of users. But they must also implement measures to improve the security of that system against both insider and outsider attacks. In general, the more users the simulator makes a student support, the more frequent the attacks and other security-related events become. If the student does not respond appropriately to mitigate the ill effects of a recent "hack", the problems will escalate to more damaging or insidious forms

of attack. In addition to attack mitigation, the simulator also exercises the proper and timely reporting of significant security events.

Ad Hoc Military Initiatives

Just-In-Time Training (JIT-T).

This method of training is completely reactionary in nature, seeking to fulfill an unanticipated, critical training requirement with whatever assets can be made available. Typically, this takes the form of hiring a vendor or consultant to provide product specific training and continuation training documentation. Subject areas normally span the install, configure, and maintain spectrum of operations. This type of training seldom maintains duration of more than three days, and requires the student/technician to assimilate vast amounts of data in short time periods. Time restrictions inherent to JIT-T prevent an integrated systems approach, reducing its applicability to CND operations. Additionally, the cost to obtain JIT-T from a vendor is at a premium. Contracting a vendor or consultant on a no-notice basis is the most expensive form of training available. It should be recognized however, that disciplined and deliberate planning of training requirements should all but eliminate the need for JIT-T. Just-in-time training has been used by the USAF to enhance CND operations in the following subject matter areas:[11]

1. Cisco Routers and Switches
2. Microsoft NT Network Operating System (NOS)
3. Microsoft Exchange Messaging
4. Sidewinder Firewalls
5. Optical Data Systems (ODS) Intelligent Switches
6. Optical Data Systems (ODS) Intrusion Detection System (CyberCop)
7. ISS RealSecure Intrusion Detection System
8. Axcent Enterprise Security Monitor (ESM)

Partnership with Industry… Knowledge Transfer.

Initiated at the discretion and needs of the local communications commander. In this training opportunity, military leadership purchases consultant expertise to live and work within the NCC or NOSC for some set period of time; typically from 6-12 months. The "hired gun" not only works the daily operations schedule like any other crewmember, but they also seek to transfer knowledge from their specific area of expertise to the military crewmembers. Partnership with Industry can support any subject matter area, from Network Operating System (NOS) optimization to defense-in-depth operations. The added benefit of this approach is the dual result of immediate task accomplishment and long term knowledge development. Ideally, the benefits of this methodology should be captured as a long-term affect. This can be accomplished if strategic-level partnerships are formalized between the military and private industry technology leaders (i.e., a contract between the USAF and IBM, Cisco, or AT&T).

On-the-Job Training (OJT).

OJT has been the cornerstone of CND training opportunities since the inception of the network centric warfare construct. It is employed at every Air Force installation as the premiere training methodology. OJT subjects leadership to minimal burdens for requirements development, training procurement, and skills management. In essence, almost the entire burden is placed upon the individual. Additionally, in an era of continuously diminishing resources this methodology is incorrectly viewed as cost effective. Although the initial financial outlays are minimal in comparison to other training opportunities, the breadth, depth, and consistency of the training are marginal; producing short-term remedies for simple requirements. However, OJT can effectively and rapidly fill holes in validated requirements, albeit for only limited duration and scope. Its primary constraint is that it can not address complex subject matter requirements.

As a result, over reliance on OJT has hindered the deployment of a defense-in-depth capability and limited the breadth of experience throughout the CND workforce.

Notes

[1] United States Air Force Concept of Operations, *USAF Concept of Operations for Information Operations*, 23 December 1999, 6-11 and 34-37.

[2] Ibid., 34.

[3] Air Force Communications Agency, *IA/IP Training in Support of O/PTN*, 11 January 2000, n.p.; on-line, Internet, 21 January 2000, www.afca.scott.af.mil/ip/sate/citsbip/citsbip2.htm.

[4] Sandra Gittlen, "Web Attackers Run Roughshod", *Network World*, Volume 17, Number 7, 14 February 2000, p10.

[5] Air Force Communications Agency, *Network Management Training Tracks*, 22 April 1998, n.p.; on-line, Internet, 17 November 1999, wwwafca.scott.af.mil/gc/gcl/optn/operate/rules/33115v2.htm.

[6] Rebecca Wetzel, "Who'll Care for Your Intranet", *Network World*, 2 June 1997, n.p.; on-line, Internet, 10 December 1999, www.nwfusion.com/netresources/o602isp.html.

[7] Robert Chatham, "Staff for Rent", *CIO Magazine*, 1 January 1998, n.p.; on-line, Internet, 10 December 1999, www.cio.com/archive/010198_forrester_print.html.

[8] Trident Data Systems, *Training Courses*, 1999, n.p.; on-line, Internet, 12 November 1999, www.tds.com/training/ida.htm.

[9] ibid., www.tds.com/training/nad.htm.

[10] Lawrence Livermore National Laboratory, *The Computer Security Training Center*, 1999, n.p.; on-line, Internet, 12 November 1999, www.ciac.llnl.gov/cstc/iebt/iebt.html.

[11] Headquarters Air Combat Command, *Networks Division War Report*, December 1998.

Part 4

Analysis

This analysis will detail the deficiencies in USAF CND operations resulting from incorrectly derived training requirements and the inappropriate selection of training opportunities to fulfill those requirements. It also develops recommendations to correct those deficiencies currently impeding the CND mission by applying a two part methodology: developing CND training requirements that are skill-based, vice job task oriented; and satisfying those skill-based requirements with training opportunities via a disciplined synchronization process. CND operators are not being properly trained with focus on the skill sets necessary to execute a seamless CND strategy. The impact of these deficiencies is mission failure.

A structured approach to CND training must be taken in order to overcome the deficiencies attributable to ad hoc processes. Validated Human Resource Management (HRM) techniques will be applied to formulate a correct training requirements process. Based on the output from the HRM processes, a training synchronization template is presented for marrying validated training requirements to training opportunities. This structured approach should be implemented as the benchmark process for applying discipline to any CND training effort. What is important in this analysis is not the output of a hypothetical training plan, but rather the adherence to an appropriate and validated training process.

Gap Analysis – Incorrectly Derived Requirements

Although there appears to be a sufficient quantity of requirements to direct and focus CND training efforts, a closer analysis of these requirements reveals deficiencies in both depth of detail and in the congruence of the underlying process. These deficiencies are a result of employing a requirements development process that follows an inappropriate methodology relative to the nature of CND work.

Analysis of Military Requirements:

A review of the military requirements for CND operations, i.e., Joint Doctrine and AF Doctrine, reveals a thorough and redundant description of the objectives, mission and responsibilities surrounding CND operations. However, it is evident that there is a complete lack of specific requirements in the areas of knowledge, skills, abilities (KSAs), job tasks, or system functions. These military requirement documents do not explicitly address the subject of training standards. This is not surprising, as this level of detail is not within doctrinal charter. What is disconcerting, however, is that the detailed training requirements have been randomly extrapolated from these doctrinal sources. The impact of random extrapolation is that any produced CND training requirements do not address the full spectrum of actual training needs. These partial and misleading lists results in training gaps and hence mission deficiencies.

The TTP document for CND attempts to establish some level of detail for training requirements, however this document only addresses CND operations on a higher, functional level. The TTP does not provide sufficient detail to develop a precise matrix of skills and job tasks. However, it does describe CND required crew positions, providing a remedial outline of job tasks and skills relevant to each crew position. These functional descriptions, although informative for basic organizational purposes, unfortunately can not in isolation support the

linkage to training requirements or training opportunity selection. They can however act as the initial step in a work analysis process.

The USAF's CND training methodology also suffers from the employment of an inappropriate requirements development process. Both the strategic (doctrinal) and tactical (job functions and skills) structures invoke a work analysis process that is job-based; describing specific tasks and criterion of the work in question. In military parlance, the work analysis produces a Mission Essential Task List (METL); it identifies what must be done. Job-based analyses that produce task lists are adequate for work that maintains relative stability against technology, but it does not lend itself to those work areas that are rapidly changing due to technology, mission requirements, or external threats[1]. CND operations maintain an intimate association with technological innovation, mission parameters, and external threats. Therefore, job-based analysis cannot adequately identify and document a useable CND METL; operational parameters are changing too fast.

Analysis of Commercial and Ad Hoc Requirements.

The identification of CND training requirements for USAF personnel is not based solely on the strategic-level assessments presented in doctrinal documents. The military also capitalizes on those CND requirements specified in both commercially available sources (e.g., text books, whitepapers, and private businesses) and from pop-up, ad hoc military needs that present themselves in USAF daily operations. The requirements derived from these sources present a much more quantifiable depth of detail; but they lack a prima facie linkage back to CND strategy, objectives or courses of action. For example, *Maximum Security* identifies the precise skills and task sequences necessary to identify and eradicate a Tear-Drop denial of service vulnerability (Tear-Drop is a method of CNA).[2] Similar task granularity can be found for a vast

spectrum of CND operational functions in any of the commercial sources. However, these skills and tasks are typically categorized into discrete and narrow subject matters and do not establish an association with CND crew positions. They are simply a collection of possible tasks … a tactical-level view of CND operations. Commercial and ad hoc requirements provide ample depth of subject matter, but are too widely dispersed, incongruent, and lacking of a unifying structure to provide feasible correlation to CND operations or crew position tasks. The use of commercial and ad hoc resources as a basis for identifying CND training requirements, absent of a unifying structure, is dysfunctional.

Gap Analysis – Inappropriate Selection of Training Opportunities

The current training methodology for USAF CND operations suffers from the inappropriate selection of training opportunities. The primary factors in this concern are synchronization against incorrect requirements, ad hoc synchronization, and over reliance on OJT.

Synchronization.

Training opportunities are proposed, programmed and utilized based on a structure of strategic and tactical-level doctrine, and commercial and daily mission influences. Operational planning concepts tell us that three levels of structure are required to move from a strategic intent to tactical action in the battlespace[3]. The Air Force's CND concept is missing the operational-level structure and guidance necessary to translate strategic missions (doctrine) into tactical actions (job functions and skills). More precisely, CND is currently deficient in course of action (COA) development and integration. Therefore, CND training opportunities are selected to address a mix of strategic and tactical requirements, absent of a unifying operational structure,

resulting in a piecemeal mission capability. Both the quality and source of CND training are of little consequence if they are married to a disjointed and dysfunctional set of requirements.

Additionally, the synchronization of training opportunities with (incorrect) requirements suffers from ad hoc application. CND operators are afforded training opportunities in no systematic or logical sequence. A review of the process that utilizes the Information Protection Operations Certification courses highlights this ad hoc methodology. This certification maintains over 120 subject matters (topics). Each topic can be studied and mastered independently. There is no intent to develop a foundation of skills or to sequence the topics together. Hence, as a training requirement presents itself, it is satisfied by a stand-alone training opportunity. This method of synchronization can not adequately sequence the COAs necessary to defeat a CNA. When an attack occurs, multiple non-related tasks must be properly sequenced in order to execute a series of defensive tactics and thus defeat the attack. If the sequence is not correctly executed then information fratricide may result. That is, an improperly trained CND operator may unintentionally disrupt mission critical information flow during their attempts to halt a CNA. Therefore, it is not the essence of CND training to seek competency in a set of independent tasks, rather it is critical to maintain expertise in a variety of tasks that can be sequenced together as an integrated COA. Synchronizing training requirements against training opportunities without regard for how the requirements will integrate into COAs does not equate to a CND capability.

On-the-Job Training (OJT).

As a stopgap measure to provide critical capabilities, which maintain an extremely short duration of usefulness, the USAF has turned to OJT as its premier training solution. Being a stand-alone process, one that ineffectively combines requirements development and opportunity

selection, OJT violates most accepted HRM principles relative to training. It relies heavily on the initiative of the individual to be trained, beyond acceptable expectations. This presents the catch-22 dilemma of the trainee not knowing what they don't know. Additionally, OJT promotes the attitude that it is appropriate to use the live network to perform training tasks that may degrade the customer's information assurance.

Improving Future Training

Delivering the CND mission demands a re-address of the CND training deficiencies that result from ad hoc requirements development and the inappropriate selection of training opportunities. The formulation of a skill-based training methodology that develops a CND operator's KSAs, vice the tasks that they must perform, is the critical cornerstone for delivering the execution of a seamless CND strategy. Additionally, the KSA requirements identified must be further refined through a disciplined process for synchronizing those requirements to training opportunities. If CND operators can successfully acquire, master, and sustain the KSAs necessary to sequence discrete tactics into integrated COAs, then training can be labeled as a success. Obtaining this objective warrants attention in two areas: requirements development via a validated HRM process and disciplined synchronization of training opportunities against those requirements. The product of these two endeavors, as depicted in Appendix A, is a flexible and cost effective training guideline, capable of keeping pace with rapid technological change.

Skill-based Process: The Cornerstone for Improving CND Training.

The cornerstone for improving the CND training methodology is identifying accurate requirements. To facilitate this effort, requirements should be developed from the bottom-up, not the top-down, using a validated HRM process. Focusing on the tactical-level of operations

will eliminate any problems resulting from a disjointed, hierarchical doctrine structure. Additionally, relationships must be established between potential CNA threats and the COAs required to thwart them. Once these relations are documented they can then be prioritized. The prioritized order of COAs will provide the focus point for applying a validated HRM process. It is from the COAs that the specific skills needed by the CND operators will be derived. The HRM process employed should support the inherent characteristics and nature of the work being scrutinized. For technology dependent jobs, the skills-based analysis process is most appropriate. A skills-based process systematically identifies and collects information about the job, spanning multiple technological platforms or traditional "stovepipe" areas of expertise[4]. The output of this process is a job specification, which identifies the KSAs necessary to perform all associated tasks. By defining the requirements as the KSAs to perform the job, instead of the tasks involved in the job, a skill-based analysis allows CND operators to train for flexible employment; moving among a wider range of tasks, thereby facilitating COA integration.

Disciplined Training Synchronization.

The first step in correctly synchronizing training opportunities to requirements is to ensure that the CND operators (i.e., potential training candidates) possess the inherent traits and characteristics that lead to a high probability of successful training. Potential CND operators should be subjected to some type of pre-training selection method; just as pilot candidates are pre-screened for certain capabilities and limitations. Not everyone maintains the capability to comprehend the intricacies of dynamic information flow or design and script computer programs. Selecting a training candidate with the traits that maintain correlation to job performance is essential.

Once the "best" potential candidates are identified, synchronization can begin, based on the prioritized COAs and resulting KSAs from the skill-based analysis. The decision to marry a certain training opportunity against a specific requirement (desired KSA) must consider at least three criteria: total cost, credible expertise, and time.[5] These criteria must be balanced to provide the greatest return on investment (ROI). Granted, mission accomplishment is still the primary consideration, but in an environment of restricted resources and funding, a program's ROI is the difference between reality and wishful dreams. The military must look to commercial industry to provide the training expertise that is inherently costly due to associations with rapidly changing infrastructures, personnel attrition, duration of applicability, and specialization. Conversely, the military should maintain some CND training capacity; specifically in the areas of basic core KSAs, where a large volume of candidates can be trained with relatively low overhead in a relatively stable area of technology (examples: network traffic analysis, Internet Protocol routing, or program scripting). Again, the key is to focus on KSAs required to perform a sequence of tasks, not the discrete tasks themselves nor the hardware/software platform that the task will be executed upon.

The following synchronization template is presented to satisfy CND training requirements. It is based on balancing the criteria of cost, expertise, and time. This template should be applied in sequential order to the training requirements identified by the skills-based process.

1. Standardized, basic military CND skills training. The Base Information Protection Ops Certification program offers training opportunities in over 120 CND subject maters. Of these, approximately 20 fundamental subject matters can be cost effectively maintained and trained as a military core capability (Appendix A). These 20 subjects maintain stability relative to technological change and do not require a deep commitment to specialization. Training requirements should be synchronized against these core CND opportunities first.

2. Augmented basic military CND training. For those areas where basic military CND training opportunities can not provide a cost-effective solution, reliance on commercial

industry is necessary. The focus here remains basic KSA development ... initial training. The vast number of commercially available training opportunities allows for two implementation strategies: centrally contracted service-wide or decentrally procured by each local base. There are a number of arguments for each case, but that is beyond the scope of this analysis. To date, the USAF has not developed a centralized business processes to collect, recommend, and publicize information pertaining to commercial consulting services necessary to assist the base-level CND training efforts.

3. On-the-Job Training (OJT). OJT should not be used as the source for acquiring basic CND skills, for it requires too much initiative on the trainees' behalf. Rather, OJT should be employed to master the skills acquired via basic military and basic commercial training through repetitive and supervised execution of daily job functions. Care must be taken not to attempt new skills development on a live network, just as a pilot wouldn't attempt a new maneuver in the middle of a refueling mission.

4. Partnership with industry. This training opportunity is used as leverage against rapid technological changes. By regularly sponsoring a CND professional from a commercial network operations center (NOC) to work alongside USAF CND operators, one can facilitate knowledge transfer and contiguous skills improvement. Additionally, knowledge transfer provides an avenue for optimizing skills proficiency through different yet complimentary operational perspectives.

5. Employ CND simulators. The utilization of CND simulators is arguably the most cost-effective training opportunity available to USAF CND efforts. First, it eliminates all risks of attempting to execute new COAs on a live network (again, refer back to the pilot analogy). Second, as new threats are identified and COAs developed, they can be rapidly programmed into the simulator; realizing that the skills necessary to execute the COA have not changed, only their combinations and sequencing have been adjusted. Third, repetitive execution of skills increases proficiency. Finally, it provides a mechanism to support the administration of crew certifications (CND operators must establish "initial" and "operational" qualifications prior to assuming responsibilities on the live network).

6. Commercial sponsored aggressor training. This is the CND equivalent of a Red Flag exercise; actual attacks against the live network. It affords the CND operator an opportunity to integrate all their available KSAs necessary to balance the competing demands of customer access and adversary denial.

7. Just-in-Time Training (JIT-T). Optimal for addressing issues pertaining to hardware/software platform migrations and unanticipated personnel attrition. Typically requires high cost layouts to retain short-notice commercial expertise. Provides training on discrete skills, vice the preferred method of skills integration. Should only be employed as method of last chance or as a critical gap-filler.

Training Product.

Once the CNA threat has been identified and prioritized, the process of acquiring training can commence. The operational-level COAs, developed to counter the CNA threats, are then examined via a skill-based analysis process. The product of this validated HRM process is a matrix of required CND knowledge, skills, and abilities (KSAs). These CND training requirements are then synchronized against available training opportunities using the cost – expertise – time criterion previously outlined in Table 7. The final result will be a contiguous and cost effective training process that accomplishes the CND mission through effective skill development and COA integration.

Notes

[1] George T. Milkovich, *Compensation* (Boston: Irwin McGraw-Hill, 1999), 59 and 144.

[2] Anonymous., *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, 1999, 344.

[3] Joint Doctrine Publication (Joint Pub 3-0), *Doctrine for Joint Operations*, 1 February 1995, II-1 to II-4.

[4] Milkovich, 82-84.

[5] "Perspectives Report", *CIO Magazine*, 29 March 1999, n.p.; on-line, Internet, 9 December 1999, www.cio.com/conferences/032999_2.html.

Part 5

Conclusion

Applying a validated HRM process to facilitate the development of CND training requirements, in combination with the disciplined synchronization of training opportunities can vastly improve the quality of CND training. This training improvement will in-turn enhance the overall mission effectiveness of CND operations, helping provide Information Assurance to the warfighter. A proper balance of military training, commercially augmented training, and employment of Information Assurance toolkits can exploit the unique benefits of each training method, while reducing their limitations and overall training costs. Additionally, the application of the correct type of HRM process will negate the draining affects that rapid technological change has on training lifecycles.

Previous CND training methodologies have inappropriately extrapolated training requirements from strategic, doctrinal guidance. This top-down approach has resulted in a task-based description of the CND work functions. These tasks, a.k.a., training requirements, are purely speculative as to what is actually necessary to defend against a CNA. They are absent of the translation and subsequent unifying logic that is provided by an operational-level COA. Individual job tasks, regardless of their validity, can not defend against a coordinated CNA; just as an individual solider, no matter how brave or skilled, can not stop an attacking armored force. Only when these individual job tasks are linked together as a cohesive and synergistic fighting

unit, via a COA, can they successfully execute the CND mission. Additionally, task-based work descriptions are susceptible to the rapid changes in today's CND technology; when the technological platform is upgraded every six months the associated job tasks must also be revisited, and thus the CND operator must be retrained.

Melding the CND requirements development process and training synchronization process into a cohesive training program requires insight through the entire CND operator lifecycle. This is not an effort that can be undertaken at the tactical-level through piecemeal and stovepipe initiatives. The effort must be driven from the operational-level. As this analysis has demonstrated, ad hoc training synchronization promotes a point-defense CND functionality; one not capable of executing the integrated and seamless COAs necessary to defeat a CNA. To gain the most benefit, the approach to CND training must acknowledge that Information Assurance is an operational art, linking strategic objectives to operational COAs.

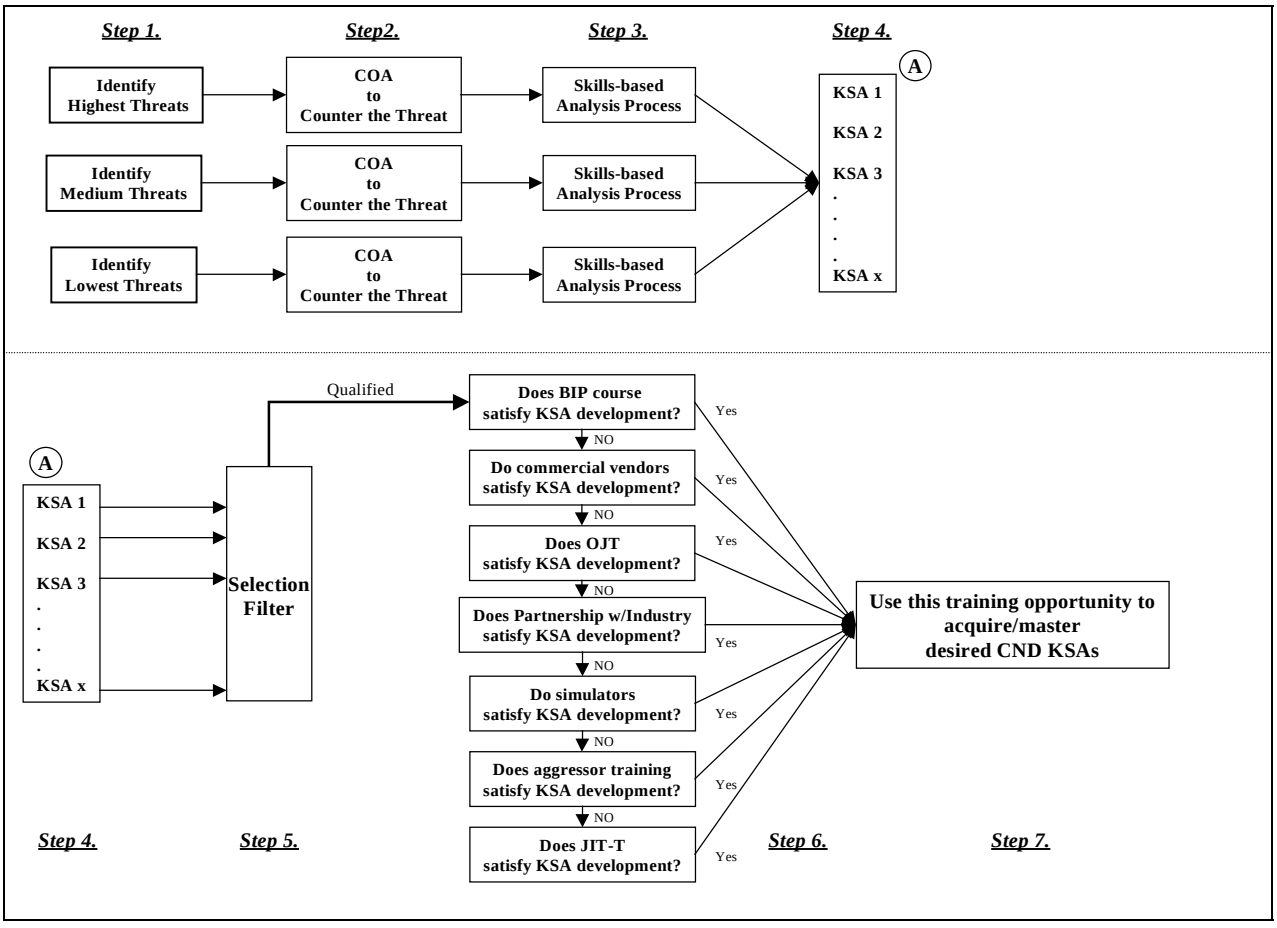
Future CND training efforts should mirror the constructs associated with pilot training: crew positions, certifications to operate, skill-based job requirements, and training that develops the operator's ability to sequence a series of discreet tasks into a seamless, unified COA. As such, CND training opportunities should employ techniques similar to those used in pilot training, including simulators, aggressor training, and requirements derived from a bottom-up approach. As is the case for the flying community, CND operations must partner with commercial industry in order to reduce costs, optimize utilization of limited manpower, and capitalize on the wealth of experience available to the private sector. One of the most promising areas for this partnership is a strategic-level agreement between the USAF and network industry leaders for tactical-level knowledge transfer. Just as a young plant's growth can benefit from being lashed

to a supporting-stake, so can an immature CND mission accelerate its operational capability by being lashed to commercial industry via knowledge transfer.

The application of validated and disciplined HRM processes to the management of CND operations presents new opportunities for cost savings, efficient utilization of manpower, and increased mission effectiveness. Information Assurance, the cornerstone of Information Superiority, must maintain an effective CND capability in order to defeat any potential adversary's CNAs. Therefore, a robust CND training process, one that is steeped in sound HRM practices, is a critical pillar to the future success of the USAF.

Appendix A

CND Training Synchronization Process



Step 1. Identify CNA threats in relative degrees of mission impact
Step 2. Develop COAs to defend against specific CNA threats
Step 3. Apply HRM skills-based analysis process
Step 4. Produce a prioritized list of KSAs required by CND operator (Training Requirements)
Step 5. Apply a selection criterion to filter out unqualified training applicants
Step 6. Synchronize training requirements to opportunities using cost/expertise/time template
Step 7. Produce a training plan for CND operators to execute prioritized COAs

Glossary

AFDD	Air Force Doctrine Document
ASIM	Automated Security Incident Measurement
BIP	Base Information Protection
C2	Command and Control
CBT	Computer Based Training
CNA	Computer Network Attack
CND	Computer Network Defense
COA	Course of Action
CONOPS	Concept of Operations
HRM	Human Resource Management
IPB	Intelligence Preparation of the Battlespace
IW	Information Warfare
IWAC	Information Warfare Applications Course
JIT-T	Just in Time Training
KSA	Knowledge, Skills, and Abilities
METL	Mission Essential Task List
NCC	Network Control Center
NOC	Network Operations Center
NOSC	Network Operations and Security Center
OJT	On-the-Job Training
OS	Operating System
ROI	Return on Investment

Bibliography

Air Force CIO. *IT Responsibilities – Training and Education*, 8 November 1999. Available from www.cio.hq.af.mil/ittrng.htm.

Air Combat Command, *Networks Division War Report*, December 1998. Available from www.networks.acc.af.mil.

Air Force Communications Agency, *IA/IP Training in Support of O/PTN*, 11 January 2000. Available from www.afca.scott.af.mil/ip/sate/citsbip/citsbip2.htm.

Air Force Communications Agency, *Network Management Training Tracks*, 22 April 1998. Available from wwwafca.scott.af.mil/gc/gcl/optn/operate/rules/33115v2.htm.

Air Force Concept of Operations (CONOPS). *Concept of Operations for Information Operations*, December 1999.

Air Force Concept of Operations (CONOPS). *Concept of Operations for the USAF Network Operations and Control Center*, October 1998.

Air Force Doctrinal Document (AFDD) 2-5. *Information Operations*, May 1999.

Air Force Manual (AFM) 3-1. *Tactics, Techniques and Procedures (TTPs) for the Operation of the Network Weapon System*, October 1999.

Anonymous. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. New York: SAMS Publishing, 1999.

Brasmahan, Jennifer. "An Interview with William Handcock", *CIO Magazine*. 19 Mar 97.

Brenton, Chris. *Mastering Network Security*. Berkeley: Sybex Inc., 1999.

Carnegie Mellon University, *Alert Statistics*, 10 December 1999. Available from www.cert.org.

Chatham, Robert, "Staff for Rent", *CIO Magazine*, 1 January 1998, n.p.; on-line, Internet, 10 December 1999. Available at www.cio.com/archive/010198_forrester_print.html.

Edwards, John. "Innovative Training Tools", *CIO Magazine*. 1 Jan 98.

Gatewood, Robert D. *Human Resource Selection.* Fort Worth: The Dryden Press, 1998.

Gittlen, Sandra, "Web Attackers Run Roughshod", *Network World*, 14 February 2000, Volume 17, Number 7.

Gralla, Preston. *How Internets Work*. New York: ZD-Press, 1997.

GTE Systems. *Introduction to Network Security and Intrusion Detection (INSID)*, 1999. Available from www.itsecure.bbn.com/insid.htm.

Holbrook, R. *Site Security Handbook, Request for Comments (RFC) 1244*, July 1991. Available from www.alw.nih.gov/Security/FIRST/papers/general/handbook.txt.

Howard, John D., *An Analysis of Security Incidents on the Internet*, 2 April 1997. Available from www.cert.org/research/JHThesis/chapter6.html.

Infowar, *The Security Store@Infowar.com,* 3 December 1999. Available from www.infowar.com.

Joint Doctrine Publication (Joint Pub) 3-13, *Information Operations*, 9 October 1998.
Joint Doctrine Publication (Joint Pub), *Joint Doctrine Capstone and Keystone Primer*, 15 July 1997.
Joint Doctrine Publication (Joint Pub) 3-0, *Doctrine for Joint Operations*, 1 February 1995.

Kaeo, Merike. *Designing Network Security*. Indianapolis: Cisco Press, 1999.

Lawrence Livermore National Laboratory. *INFOSEC Experience-Based Trainer: IEBT*. Available from www.ciac.llnl.gov/cstc/iebt/iebt.html, 1999.

Milkovich, George T. *Compensation*. Boston: Irwin McGraw-Hill, 1996.
Milkovich, George T. *Human Resource Management*. Chicago: McGraw-Hill, 1997.

Network Security Solutions Ltd. *Techniques Adopted by System Crackers When Attempting to Break Into Private Networks*. Available from www.hideaway.net/texts/cracker.txt, December 1998.

Pabrai, Uday. *Webmaster Administrator Certification Exam Guide.* New York: McGraw-Hill, 1998.
"Perspectives Report", *CIO Magazine*, 29 March 1999. Available from www.cio.com/conferences/032999_2.html.

Trident Data Systems. *Network Attack & Defend Course #3101*. Available from www.tds.com/training, 1999.
Trident Data Systems. *Intrusion Detection & Analysis Course #3105*. Available from www.tds.com/training, 1999.

Wetzel, Rebecca, "Who'll Care for Your Intranet", *Network World*, 2 June 1997, n.p.; on-line, Internet, 10 December 1999, www.nwfusion.com/netresources/o602isp.html.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112