



Calhoun: The NPS Institutional Archive

Theses and Dissertations

Thesis Collection

2001-06

Experimentation methodology for evaluating operational INFOCON implementations.

Kimmel, Richard A.

<http://hdl.handle.net/10945/10882>



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

**EXPERIMENTATION METHODOLOGY FOR
EVALUATING OPERATIONAL INFOCON
IMPLEMENTATIONS**

by

Richard A. Kimmel

June 2001

Principal Advisor:
Associate Advisor:

William G. Kemple
Shelley P. Gallup

Approved for public release; distribution is unlimited.

20010803 008

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, 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 this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2001	3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE : Experimentation Methodology for Evaluating Operational INFOCON Implementations			5. FUNDING NUMBERS
6. AUTHOR(S) Richard A. Kimmel			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A
13. ABSTRACT (maximum 200 words) Information Operation Condition (INFOCON) implementations and specifically the impact these implementations can have on warfighting command and control processes are not yet widely understood or appreciated by the majority of the operating forces. INFOCON actions are designed to heighten or reduce defensive posture uniformly, to defend against computer network attacks, and to mitigate sustained damage to the DoD infrastructure. Experimentation is required to explore the effects on certain command and control processes under various INFOCON conditions. This thesis explored requirements for conducting these INFOCON experiments and resulted in the development of an INFOCON experimental design methodology that can be used as a framework for designing and conducting INFOCON experiments in the field. INFOCON experimentation will provide insights and a better understanding of the effects that these implementations will have on the ability of a commander to command and control his or her forces.			
14. SUBJECT TERMS Command, Control and Communications, Information Operations, Information Conditions, Computer Network Defense, Experimentation			15. NUMBER OF PAGES 125
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**EXPERIMENTATION DESIGN METHODOLOGY FOR EVALUATING
INFOCON IMPLEMENTATIONS**

Richard A. Kimmel
Civilian, Naval Postgraduate School
B.S., Chapman University, 1988

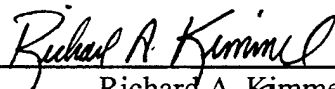
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

**NAVAL POSTGRADUATE SCHOOL
June 2001**

Author:



Richard A. Kimmel

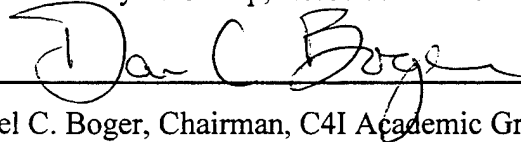
Approved by:



William G. Kemple, Principal Advisor



Shelley P. Gallup, Associate Advisor



Daniel C. Boger, Chairman, C4I Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information Operation Condition (INFOCON) implementations and specifically the impact these implementations can have on warfighting command and control processes are not yet widely understood or appreciated by the majority of the operating forces. INFOCON actions are designed to heighten or reduce defensive posture uniformly, to defend against computer network attacks, and to mitigate sustained damage to the DoD infrastructure. Experimentation is required to explore the effects on certain command and control processes under various INFOCON conditions. This thesis explored requirements for conducting these INFOCON experiments and resulted in the development of an INFOCON experimental design methodology that can be used as a framework for designing and conducting INFOCON experiments in the field. INFOCON experimentation will provide insights and a better understanding of the effects that these implementations will have on the ability of a commander to command and control his or her forces.

TABLE OF CONTENTS

I. INTRODUCTION.....	1
A. BACKGROUND	1
B. PURPOSE.....	4
C. RESEARCH QUESTIONS	5
D. ORGANIZATION OF STUDY	5
II. C4I SYSTEMS SECURITY IN A NETWORK CENTRIC ENVIRONMENT: AN OVERVIEW	7
A. THE SHIFT TOWARDS NETWORK CENTRIC WARFARE.....	7
1. Information Superiority	7
2. Potential Impact Of C4I On Military Operations.....	9
3. Information Operations/Information Assurance	9
4. Information Assurance Operations	11
B. SECURITY IMPLICATIONS FOR NETWORK CENTRIC WARFARE	12
1. Information Security Organizational Culture.....	13
2. Network Centric Warfare Is Technology Based	13
3. Network Centric Warfare Is Information Intensive	14
C. INFORMATION SYSTEM SECURITY	15
1. Major Challenges To Information Systems Security	15
a. Networked Systems	16
b. The Asymmetry Between Offensive And Defensive Information Warfare Security	16
2. Defensive Functions	17
a. Monitor Indications And Warnings.....	17
b. Plan A Range Of Responses.....	18
III. INFORMATION OPERATIONS CONDITION SYSTEM.....	21
A. PURPOSE.....	21
B. INFOCON SYSTEM DESCRIPTION	22
C. LEVELS AND CRITERIA.....	23
D. RESPONSIVE MEASURES	25
E. INFOCON IMPLEMENTATION PROCESS.....	26
F. KEYS TO SUCCESSFUL IMPLEMENTATION OF THE INFOCON SYSTEM	27
1. System Interface Description.....	27
2. System Communications Description	29
3. Operational Node Connectivity Description.....	30
G. SUMMARY.....	32
IV. SPAWAR IO C2 EXPERIMENT: THE IMPACT OF INFOCON LEVELS ON SIMULATED FLEET OPERATIONS.....	35
A. EXPERIMENT OVERVIEW	35
1. Operational Background.....	35
2. Objective	38
3. Scientific Background	39
a. Workload Measurement.....	39
b. Situational Awareness Measurements	40
B. EXPERIMENT DESIGN	42
1. Experiment Architecture.....	42
a. Experimental Unclassified Network.....	45
b. Experimental Secret Network.....	46
2. Experiment Participants.....	47
a. Test Subjects	47

b. Observers	48
c. Subject Matter Experts (SME's).....	48
3. Role-Based Functionality	49
4. Variables.....	50
5. Procedure.....	50
6. Tasks.....	53
C. RESULTS.....	57
1. Workload Impact.....	57
2. Situational Awareness.....	58
3. Time Delta	59
4. Lessons Learned	60
V. INFOCON FIELD EXPERIMENTATION METHODOLOGY	63
A. FIELD SETTING OVERVIEW	63
1. Exercises Versus Experiments.....	63
2. Laboratory Experiment To Operational Environment	64
B. MODULAR COMMAND AND CONTROL EVALUATION SYSTEM.....	65
C. INFOCON PROBLEM FORMULATION	66
1. Example INFOCON Field Experiment Objective	68
2. Example INFOCON Experimental Questions	68
D. INFOCON SYSTEM BOUNDING AND PROCESS IDENTIFICATION	69
1. Understanding The C4I Architecture, Information Flow And Integration Details.....	70
2. Relationship Between Human Factors And Organizational Issues	71
E. INFOCON SCENARIO SPECIFICATION AND SELECTION ISSUES	72
F. INFOCON MEASURES OF MERIT	74
1. Impact Of Infocon On Mission Performance.....	75
2. INFOCON Workload Assessment With NASA Task Load Index	76
3. Relationship Between INFOCON And Situational Awareness	77
4. Instrumentation.....	78
G. DATA COLLECTION AND ANALYSIS STRATEGY.....	79
VI. SUMMARY	83
APPENDIX A. JCS INFOCON MEMORANDUM.....	89
APPENDIX B. INFOCON STRUCTURE.....	91
APPENDIX C. COMTHIRDFLT INFOCON STANDARD OPERATING PROCEDURES	93
APPENDIX D. WORKLOAD INSTRUMENTS.....	97
APPENDIX E. IA C2 EXPERIMENT DESIGN AND DATA COLLECTION FLOW	103
LIST OF REFERENCES.....	105
INITIAL DISTRIBUTION LIST	107

I. INTRODUCTION

In the last two years we have seen a series of intrusions into numerous Department of Defense computer networks as well as networks of other federal agencies, universities, and private sector entities. Intruders have successfully accessed U.S. Government networks and taken enormous amounts of unclassified but sensitive information. (Louis J. Freeh, Director, Federal Bureau of Investigation, 16 February 2000)

A. BACKGROUND

Unauthorized access to Department of Defense (DoD) computer networks and systems poses a real and current potential threat to our national security. From the acquisition of information to the disruption of activities during critical operational periods, computer system and network intrusion and attack represent significant derivative vulnerabilities of the DoD's reliance on information systems and information technology in the conduct of daily business. Louis J. Freeh, Director, Federal Bureau of Investigation, stated:

One of the greatest potential threats to our national security is the prospect of 'information warfare' by foreign militaries against our critical infrastructures. Foreign nations are developing information warfare programs because they cannot defeat the United States in a head-to-head military encounter and they believe that information operations are a way to strike at America's Achilles Heel - our reliance on information technology (Freeh, 2000)

The government's increased worldwide dependence on information technologies and the vulnerabilities associated with this dependence for military operations demands

protection, detection, restoration, and an integrated response to protect and defend friendly information and systems from attack.

The Chairman of the Joint Chiefs of Staff Memorandum, CM-510-99, dated 10 March 1999, established the Information Operations Condition (INFOCON) system for DoD. The intent of the INFOCON system is to provide all DoD elements with a structured, standardized approach to defend against and react to attacks on computer systems and networks. Initially, the Director for Operations, Joint Staff (J3) was responsible for administering the INFOCON system. This transitioned to the Commander of the Joint Task Force for Computer Network Defense (JTF-CND) as this new task force reached initial operational capability. On 1 October 1999, Commander in Chief, U.S. Space Command assumed responsibility for computer network defense including command authority over JTF-CND.

INFOCON actions are designed to heighten or reduce defensive posture uniformly, to defend against computer network attacks (CNA), and to mitigate sustained damage to DoD infrastructure. There are currently five INFOCON levels that reflect defensive postures based on the risk or existence of computer network attacks. The following provides a general characterization of each INFOCON level:

NORMAL - There is no significant activity indicating an increased risk of attack

ALPHA - There is an increased risk of attack

BRAVO - There is a specific risk of attack

CHARLIE - A limited information system attack has been detected

DELTA - Information systems are under attack

The dynamics of INFOCON implementations, and specifically their impact on the ability of warfighters to execute command and control functions effectively, are not yet widely understood and/or appreciated by the majority of the operating forces. Naval staffs at the Numbered Fleet level and above have been working coordination and implementation issues associated with INFOCON's since well before CM-510-99 articulated the current INFOCON policy, and INFOCON actions are now being incorporated in Fleet training exercises. However, specific policy and actions to make INFOCON implementation an effective tool in protecting the vital information infrastructure of the DoD are still under development. The concepts, responsive measures, and impact of responsive measures are still exploratory and require focused experimentation efforts to gain further understanding. Because military command and control networks are truly global in nature, actions taken at one location in response to operational and intelligence assessments resulting in INFOCON decisions have far reaching and at times not fully understood effects in a network centric environment.

The critical role of global networks to support naval operations makes the development of effective infrastructure protection of the utmost importance to naval forces. The INFOCON system provides all DoD elements with a structured, standardized approach to defend against and react to attacks on computer systems and networks. INFOCON actions should be reviewed and tested often. This will help personnel understand their roles and responsibilities, determine the effect of responsive measures on mission effectiveness, and detect problems in existing procedures. As an initial step to understanding INFOCON concepts, a controlled experiment, in which the author

participated, was conducted at the SPAWAR Information Operations Center of the Future (IOCOF) laboratory in May, 2000 with a COMTHIRDFLT Battle Watch Staff. This effort identified important baseline information relating to situational awareness (SA) and command and control effectiveness. Although much was learned from this early effort, the test environment was artificial. Therefore, subsequent experimentation in an operational environment is needed to better understand the impacts that setting INFOCON's will have on "real world" mission tasking. Specifically, INFOCON experimentation in an operational environment should be conducted to better understand the impact of INFOCON implementations on the command and control process.

B. PURPOSE

As mentioned above, Information Operation Condition (INFOCON) implementations and specifically the impact these implementations can have on warfighting command and control processes are not yet widely understood or appreciated by the majority of the operating forces. Experimentation is required to explore the effects of imposing INFOCON on command and control functions in an operational environment under various scenarios. This thesis will explore requirements for conducting these INFOCON experiments and will result in the development of an INFOCON experimental design methodology that can be used as a baseline for conducting operational INFOCON experiments.

C. RESEARCH QUESTIONS

A primary hypothesis associated with INFOCON implementation is that the increasingly restrictive posture associated with progressive INFOCON levels will have a correspondingly adverse impact the warfighters' ability to accomplish command and control tasks in a network centric environment. In order to obtain data to examine this hypothesis, experimentation aimed at researching the effects on certain command and control processes under various INFOCON conditions is required. INFOCON experimentation efforts will provide insight and a better understanding of the effects that these implementations have on the ability of a commander to conduct seamless command and control functions after such conditions are instituted. This thesis will result in the development of an experiment design framework that one can use for evaluating the effects of imposing INFOCON on operational command and control functions. The primary questions to be researched in this thesis include:

- How can the effects of INFOCON be evaluated in an operational environment?
- What is the baseline INFOCON experimental design for measuring the impact of INFOCON implementations on an operational command and control architecture?

D. ORGANIZATION OF STUDY

This thesis is divided into six chapters including the introduction. Chapter II, C4I Systems Security in a Network Centric Environment: An Overview, provides a synopsis of the Network Centric Warfare concept and discusses the requirements and challenges of maintaining information dominance in a Network Centric Warfare environment. In

addition, this chapter also provides a broad overview of issues related to computer network vulnerabilities and includes a discussion of the difficulties associated with protecting military networks from an adversarial attack. Chapter III, Information Operation Condition (INFOCON) System, is intended to provide the reader with a thorough understanding of the INFOCON concept. It also highlights several recent INFOCON exercise and experimentation efforts and documents key lessons learned from those efforts. Chapter IV, Information Assurance (IA) Command and Control (C2) INFOCON Lab Experiment, provides a detailed description of the IA C2 experiment, in which the author participated. It includes sub-sections describing the experimental design, data collection methodology, data analysis approach, and lessons learned. These sub-sections will be used as a guide from which a framework for conducting an experiment in an operational environment will be based. Chapter V, INFOCON Field Experimentation Methodology, will provide experiment planners with the methodology and tools necessary for planning and conducting an INFOCON experiment that focuses on the impact to command and control processes in the midst of varying INFOCON levels. This section will detail how an operational INFOCON experiment can be conducted and will provide the framework to shape an experiment for various operational scenarios. Rather than design a rigid experiment focused on a specific command and control architecture, this approach provides the essential focus areas that planners must consider prior to planning and conducting an INFOCON experiment.

II. C4I SYSTEMS SECURITY IN A NETWORK CENTRIC ENVIRONMENT: AN OVERVIEW

A. THE SHIFT TOWARDS NETWORK CENTRIC WARFARE

Information and knowledge have always been crucial in warfighting, but operational and organizational innovation, supported by emerging technology, now has the potential to produce orders of magnitude improvements in our ability to build superior knowledge and then exploit this superiority for decisive success. The Navy Capstone Concept articulates how the Navy will shift from attrition-based, platform centric operations to effects-based, network centric operations. This concept known as Network Centric Warfare (NCW) says that as we fight a brown water (littoral) battle, we need to connect our ships, weapons systems, information systems and intelligence systems in a network centric manner, much like we use the Internet to connect a variety of users to a common backbone. NCW leverages knowledge and information to operate inside potential adversaries' sensor and engagement timelines and to create a disproportionate impact on potential adversaries in presence, crisis and war.

1. Information Superiority

Throughout history, successful military operations and warfare have depended upon timely and accurate information. In the age of digital electronics, our forces rely upon computers and telecommunications as essential information components of all types of defense systems and functions. These information capabilities are vital to achieving

Information Superiority – the key to our Joint Vision 2010 (JV2010) goal of Full Spectrum Dominance. JV2010 provides a conceptual template established to improve the conduct of joint warfighting operations by leveraging technological advances. JV2010 introduced the emerging operational concepts of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimensional Protection. The key enabler for all four of these operational concepts is Information Superiority based on the ongoing revolution in technological development. Without Information Superiority, JV2010's concepts become little more than the current operational concepts of maneuver, strike, protection, and logistics. In short, without Information Superiority, the U.S. military will lose its edge and find itself fighting the protracted wars of attrition JV2010 was designed to preclude.

Joint Vision 2010 also stresses the importance of Information Superiority as the basis for improved command, control, and intelligence functions. Information Superiority is defined in Joint Publication 3-13, Joint Doctrine for Information Operations, as “the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying and adversary’s ability to do the same.” (Joint Pub 3-13, 1998) Thus, by definition, Information Superiority has both defensive and offensive implications. In order to achieve an uninterrupted flow of information, the systems and processes that enable that flow must be defended against adversarial actions. Although degrading an adversary’s information flow is important, defending one’s own is even more critical to successful military operations.

2. Potential Impact of C4I on Military Operations

To exercise authority and direction effectively in combat and other military operations, commanders must have situational awareness. Understanding the battlespace is essential to the command and control of the forces. The cornerstone of information superiority is advanced C4I technology and systems, which can provide to all tactical levels of command a robust, continuous, common operating picture of the battlespace. The resulting heightened situational awareness should vastly improve the effectiveness with which commanders at all levels can pursue a mission.

However, DoD is in an increasingly compromised position. The rate at which information systems are being relied on outstrips the rate at which they are being protected. Also, the time needed to develop and deploy effective defenses in cyberspace is much longer than the time required to develop and mount a cyberspace attack. According to the National Research Council (NRC) study, Realizing the Potential of C4I: Fundamental Challenges, “The result is vulnerability: a gap between exposure and defense on the one hand and attack on the other. This gap is growing wider over time, and it leaves DoD a likely target for disruption or pin-down via information attack.” (NRC, 1999) Hence, the more military leverage that C4I systems provide for U.S. forces, the larger the incentives are for an opponent to attack those systems.

3. Information Operations/Information Assurance

The process of attacking and defending information is Information Operations (IO), defined in DoD Directive 3600.1, Information Operations, as “action taken to affect

adversary information and information systems while defending one's own information and information systems." (DoD 3600.1, 1998) This definition communicates that there is more to IO than simply attacking computer systems. IO consists of technology, processes, and human factors impacting the mind of the decision-maker. IO can be targeted against leaders or key decision-makers, but can also affect every echelon of the military, government, and even the general population.

According to Joint Publication 3-13, Defensive Information Operations "ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes." (Joint Pub 3-13, 1998) Defensive IO are conducted through Information Assurance (IA), Operational Security (OPSEC), physical security, counter deception, counter psychological operations, counter intelligence, and electronic warfare. Although each of these actions is important, Information Assurance is the most critical to the success of the operational concepts described in JV2010 because it ensures that friendly systems will provide the information as required and that friendly systems are protected or isolated from potential adversarial attack. Information Assurance (IA) is defined in Joint Publication 3-13 as:

Information Operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Joint Pub 3-13, 1998)

4. Information Assurance Operations

Information Assurance (IA) actions are IO that incorporates detection, protection, and reaction capabilities to protect and defend information and information systems by ensuring the security services of: availability, integrity, identification and authentication, confidentiality, and non-repudiation. The Information Operation Condition (INFOCON) system is a proactive IA initiative that recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to the DoD information infrastructure, including computer and telecommunications networks and systems. Details of the INFOCON system are discussed in Chapter III.

IA policy drives IA operations by establishing goals, courses of action, and standards. IA policy formally states the security requirements for information systems, what must be protected, how resources are used, and what must be done or not done during situational threat scenarios. Standard operating procedures (SOP) should define system configuration, deployment, routine operations, and incident response and reporting details.

As an example, after an intrusion is detected, incident information must be reported through established channels to appropriate authorities and specialized analysis and response centers. Incident response begins with immediate local emergency damage-limitation and survivability actions that should be stated in the SOP and implemented promptly. As mentioned in Information Assurance Through Defense in Depth, a paper

prepared for the Joint Staff by Lt Col B. Ashley, USAF, "Careful, effective and timely decisions must be made concerning appropriate additional responses, such as: declare a higher level security situation or information condition (INFOCON), isolate affected systems, or pursue legal, diplomatic, economic, or military actions." (Ashley, 1999)

B. SECURITY IMPLICATIONS FOR NETWORK CENTRIC WARFARE

DoD's increasing reliance on information technology in military operations increases the value (to an adversary) of DoD's information infrastructure and information systems as a military target. Thus, if the United States is to realize the benefits of increased use of C4I in the face of a clever and determined opponent, it must secure its C4I systems against attack. Traditionally, the military has ensured the security of its information systems by a risk avoidance strategy. That is, keeping its network infrastructure separate from the public Internet, and strictly limiting access to it via locked spaces, security clearances, and cryptographic devices. However, the drive to attain Network Centric Warfare capability has profound implications for security and requires a shift in the protection strategy. In a June 1999 address to the Senate Governmental Affairs Committee, Lt General Kenneth A. Minihan, then Director National Security Agency, stated:

We face increasing risks to U.S. interests in cyberspace. U.S. dependence on, and worldwide connectivity through this relatively new medium increase our exposure to traditional adversaries and a growing body of new ones, many of whom are fast developing their capabilities to exploit and disrupt networked information systems. The ability of adversary groups and nation states to disrupt or influence U.S. civil and military activities through manipulation of our information networks, without having to confront directly traditional U.S. military power, will become an increasingly attractive option for them as we move through the 21st century. (Minihan, 1999)

1. Information Security Organizational Culture

The National Research Council (NRC) study, Realizing the Potential of C4I: Fundamental Challenges, emphasizes, “A culture of information security is required throughout the organization. The culture of any organization determines how seriously its members take their security responsibilities. For information security, policies and practices are at least as important as technical mechanisms.” (NRC, 1999) The study also indicates that senior leadership must take the lead to promote information assurance as an important cultural value. Top-level commitment is not sufficient to ensure good security practices. Without it, however, the organization will not focus on security but will expend its energy on other things that seem more directly related to its core mission.

2. Network Centric Warfare is Technology Based

The Naval Operations In the Information Age – A Capstone Concept for Network Centric Operations paper clearly identifies and discusses the value of Network Centric Warfare enabled by the achievement of Information Superiority. The Navy’s IT-21 initiative was designed and implemented to achieve this Information Superiority in a time

of limited resources and rapidly changing technology by requiring that the military capitalize on available commercial off-the-shelf (COTS) technology as much as possible. However, the combination of open standards, COTS technology, full connectivity, and information service regionalization has compelled the military to develop a new protection strategy based not on risk avoidance, but rather on risk management. We now embrace common technologies, recognizing that some of these technologies come with well-documented vulnerabilities. Further, as more and more systems are interconnected, the user population increases significantly. The sharing of a common infrastructure which connects with the public Internet brings with it a world-wide host of hackers, criminals and foreign agents who are practiced and capable of surfing their way through that infrastructure.

3. Network Centric Warfare is Information Intensive

Traditionally, security has focused on ensuring confidentiality; the non-disclosure of classified information to those who are not authorized to see it. While this remains an important consideration, the shift to Network Centric Warfare, with its goal of speed of command, is heavily reliant on both the accuracy and timeliness of information, and on the continued availability of critical communication channels. A military maneuver is not likely to succeed if its participants cannot communicate, or if their decisions and actions are based on inaccurate, false, or outdated information. Many of the best known and most common attacks that occur on the Internet are those that target information integrity (e.g. viruses) or seek to bring down a system (e.g. flooding attacks). Some attacks, such

as Internet Protocol (IP) spoofing, focus on masquerading that can result in planting false information. Other attacks such as corrupting the translation tables of a Domain Name Server can cut off or hijack communication channels. Thus, the protection strategy for today's military operations must address not only confidentiality, but also the integrity, authenticity and timeliness of information, and continued availability of processing and communications capabilities. In addition, independent units must be acquainted with the fundamentals of information security procedures as they pertain to a potential attack of the systems on their platform. In the event of an information attack, individual units must understand what they should do and how those actions will impact the command and control process during the current mission.

C. INFORMATION SYSTEM SECURITY

1. Major Challenges to Information Systems Security

Maintaining the security of DoD C4I systems is a problem with two dimensions. The first dimension is physical. That is protecting the computers and communications links as well as command and control facilities from being physically destroyed or jammed. For this task, the military has a great deal of relevant experience that it applies to systems in the field. For example, the military knows to place key C4I nodes in well-protected areas with guards and other access control mechanisms in place to prevent sabotage, if required. However, information systems security, the other dimension, is a much more challenging task. Information systems security, the task of protecting the C4I systems connected to the communications network against an adversarial attack is much

more poorly understood than physical security. The issue of protecting DoD C4I systems against attack is complicated by the fact that many military C4I systems are interconnected with the civilian infrastructure. DoD is thus faced with the problem of relying on components of an infrastructure over which it does not have control.

a. Networked Systems

The utility of an information or C4I system generally increases as the number of other systems to which it is connected increases. However, increasing the number of connections of a particular system to other systems also increase its vulnerability to attacks routed through those connections. This is especially true when information systems are networked through the Internet. It is desirable to use the Internet because it provides lower information transport costs than the public switched telephone network or dedicated systems. However, the use of the Internet to connect C4I systems poses special vulnerabilities and currently provides neither quality-of-service (QOS) guarantees nor good isolation from potentially hostile attacks.

b. The Asymmetry Between Offensive and Defensive Information Warfare Security

According to Dorothy Denning, author of Information Warfare and Security:

Information warfare consists of offensive and defensive operations against information resources of a "win-lose" nature. It is conducted because information resources have value to people. Offensive operations aim to increase this value for the offense while decreasing it for the defense. Defensive operations seek to counter potential losses of value. (Denning, 1998)

Information systems security is fundamentally a defensive function and as such suffers from an inherent asymmetry between cyber attack and cyber defense. Because cyber defense requires an organization to always be on guard, as opposed to the cyber-attack which can be conducted at the discretion of the attacker, it is often more expensive to implement a defensive posture and requires enormous amount of effort to eliminate security flaws and implement policy/procedure (e.g. INFOCON) aimed at immediate protection of resources and deterring an adversarial attack. In short, a successful defender must be successful against all attacks, regardless of where the attack occurs, the type of attack, or the time of the attack. In contrast, a successful attacker has only to succeed in one place at one time with one technique to create a potentially damaging impact on a critical operation.

2. Defensive Functions

A number of defensive functions must be performed in an effective and coordinated fashion to ensure that information security is being taken seriously and conducted effectively. These functions include:

a. Monitor Indications and Warnings

All defenses (physical and cyber) rely to some extent on indications and warnings of impending attack. The reason is that if it is known that attack is impending, the defense can take actions to reduce its vulnerability and to increase the effectiveness of its response. This function calls for:

- *Monitoring of threat indicators.* For example, near simultaneous penetration attempts on multiple military information systems may reasonably be considered an indication of an orchestrated attack. The notion of an Information Condition (INFOCON) would be a useful summary device to indicate to commanders the state of cyber-threat at any given time. INFOCON's provide a set of pre-established measures to assess threats against information systems and define graduated actions to be taken in response to those threats. INFOCON's are roughly analogous to the defense condition (DEFCON) and terrorist condition (THREATCON) levels. The decision to change the INFOCON level is based on the assessed threat, the capability to implement the required protective measures, and the overall impact the action will have on an organizations capability to perform its mission. INFOCON's define appropriate information operations measures to be taken and are designed to produce detection, assessment, and response measures commensurate with the existing threat indicators. Chapter III discusses the details of INFOCON system implementations.
- *Dissemination of information about the threat.* Knowledge of the techniques used in an attack on one information system may enable administrators responsible for other systems to take preventive actions tailored to that type of attack.

b. Plan a Range of Responses

Organizations relying on information systems should have a number of routine information system security activities, e.g. security features that are turned on and security procedures like INFOCON's that are followed. Tailoring in advance a range of

information systems security actions to be taken under different threat conditions would help an organization plan its response to any given attack. Further understanding the impact that implementing these specific security actions (e.g. INFOCON's) will have on command and control processes will permit commanders to more effectively maneuver during cyber threat conditions.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INFORMATION OPERATIONS CONDITION SYSTEM

A. PURPOSE

Today, advanced U.S. information technology provides a decisive advantage to U.S. military forces through the integration of sensors, command and control systems, and weapon systems. Joint Vision 2010 articulates the future strategic importance of Information Superiority. This strategic importance brings with it the security vulnerabilities associated with information technology. DoD organizations present opportune targets for attack on information infrastructures. A host of potential adversaries, including novice computer hackers, disgruntled employees, non-state actors, and nation-state-sponsored organizations can exploit any information vulnerabilities. The existence of these information vulnerabilities demands an aggressive defensive Information Operation (IO) and Information Security (INFOSEC) strategy to ensure combat readiness.

The Information Operations Condition (INFOCON) system recommends actions to uniformly heighten or reduce defensive posture to defend against computer network attacks and to mitigate sustained damage to the DoD information infrastructure, including computer and telecommunications networks and systems. It provides a comprehensive defensive posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system impacts all personnel who use DoD information systems. It protects

systems while supporting mission objectives, and coordinates the overall defensive effort through adherence to standards.

B. INFOCON SYSTEM DESCRIPTION

Chairman Joint Chiefs of Staff (CJCS) Memorandum CM-510-99, Appendix A, dated 10 Mar 1999, established INFOCON for the DoD. As implied above, the intent of the INFOCON system is to provide all DoD elements with a structured, standardized, coordinated approach to defend against and react to adversarial attacks on DoD computer and telecommunications networks and systems. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and standoff capability make computer network attack (CNA) an attractive option for our present adversaries. The INFOCON system describes increasing threat activities and the corresponding responses to defend against CNA and mitigate damage to the DoD information infrastructure. Appendix B, INFOCON Structure, supplied by the JTF-CND organization, provides criteria for the various INFOCON levels and is designed to assist decision-makers with appropriate response actions based on the perceived threat. Although INFOCON implementations chiefly focuses on the CNA aspect of Information Operations, the DoD INFOCON criteria and response actions may be expanded at a later date to include all forms of information operation conditions.

C. LEVELS AND CRITERIA

Three broad categories of factors influence the INFOCON: operational, technical, and intelligence. Changes to the INFOCON level are based upon significant changes in one or more of these categories. Some of the specific factors that may be considered when determining the INFOCON include the current world situation, a commander's assessment of the potential for an information attack, current/planned military operations, Information Assurance Vulnerability Alert (IAVA) bulletins, and operational impact assessments.

Detailed INFOCON discussions with Ms. Regina Walker, a Computer Scientist assigned to the Operations Directorate in the Joint Information Operations Center (JIOC), indicate that five INFOCON levels currently exist. She stated that:

The INFOCON system provides a standard and systematic approach to deal with the increasing problem of attacks on DoD networks. The five levels indicate the likelihood or severity of attack and provide guidance on what responsive measures should be implemented. While it is important that the appropriate INFOCON is declared, the ultimate success of the system depends upon thorough planning and rehearsal to best understand the implications that a particular INFOCON response will have on a specific command and control process. (Walker, 2000)

Chief of Naval Operations message (181840Z May 99), Navy Information Operations Condition (INFOCON) Implementation, describes the five INFOCON levels as the following: (refer to Appendix B for a detailed description of the five INFOCON levels).

- **NORMAL:** There is no significant activity indicating an increased risk of attack. All mission-critical information on information systems and their operational importance should be identified. Points of access and their operational necessity should also be identified. Personnel should conduct normal security practices for their information systems, such as periodically reviewing and testing higher level INFOCON actions.
- **ALPHA:** There is an increased risk of attack. Criteria for declaring this level include indications and warnings indicating a general threat, actions indicating a pattern of surveillance of information systems, and a military operation requiring increased security of information systems. Recommended response actions include increasing the application of general security practices, such as conducting an internal review of all critical systems.
- **BRAVO:** There is a specific risk of attack. Criteria to consider before declaring this level include a network penetration or denial of service with no impact to DoD operations. Recommended response actions include increasing the application of general security practices, such as disconnecting unclassified dial-up connections not required for current operations.
- **CHARLIE:** A limited information system attack has been detected. Criteria to consider before declaring this level include intelligence assessments indicating a limited attack and an information system attack with limited impact on DoD operations. Recommended response actions include re-routing mission-critical

communications through unaffected systems and disconnecting non-mission-critical systems from networks.

- **DELTA: Information systems are under attack.** There may be widespread incidents that undermine a system's ability to function effectively and result in a compromise and significant risk of mission failure. Recommended actions include isolating compromised systems from the rest of a network and implementing procedures for conducting operations in a stand-alone mode or manually.

D. RESPONSIVE MEASURES

Responsive measures associated with INFOCON's are normally recommended actions unless specifically directed by the Secretary of Defense (SECDEF). These measures should be commensurate with the risk, an adversary's assessed capability, and intent and mission requirements. Dorothy E. Denning, a Professor of Computer Science at Georgetown University, highlights examples of CNA responsive measures in her book, Information Warfare and Security. She explains that:

Several responsive measures associated with INFOCON implementations include isolating the affected network segment, blocking offending Internet Protocol (IP) addresses, recalling key information system security personnel, updating virus signature files, running virus detection/eradication software, and isolating compromised portions of affected systems. (Denning, 1998)

She adds, "it should be noted that each responsive measure mentioned would have an impact on the flow of information and thus effect command and control in some capacity. It is the implementation of each responsive measure and a complete

understanding of the effects that each response will have on specific decision making processes that must be explored and documented." (Denning, 1998)

Ideally, computer network defense (CND) operations will be based on some advanced warning of an attack. For example, according to subject matter experts on the Commander Third Fleet (C3F) staff, "the intelligence community is developing a capability to provide CNA warning which will become of increasing value as it matures. This warning will provide a means for a commander to better assess the responsive measures needed to counter a hostile threat condition." There is a balancing act, however. Over-aggressive countermeasures may result in self-inflicted degradation of system performance and communications ability, which may ultimately contribute to the adversary's objectives. Commanders must also consider the impact that imposing a higher INFOCON for their command will have on connectivity with computer networks and systems of other commands. Although the commander has the final judgment for declaring an INFOCON posture, objective assessment of the situation and prudent analysis of all available objective information must be integrated with the commander's experience and leadership to determine the organization's appropriate defensive posture.

E. INFOCON IMPLEMENTATION PROCESS

The INFOCON system is administered through the Joint Task Force - Computer Network Defense (JTF-CND), which was subordinated to USCINCSpace on 1 Oct 99. Notification of a change in INFOCON status is disseminated from the JTF-CND to combatant commands and agencies. The commands and agencies are then responsible

for notifying units assigned to them of impending change. This notification includes the recommended or directed responsive measure.

Commanders or Directors may change the INFOCON of their organizations but conditions implemented must remain at a level commensurate with the current INFOCON direction from the JTF-CND. Ms. Walker (JIOC J3) commented that:

when commanders consider imposing a higher INFOCON for their command, they should consider the impact their decision may have on connectivity with information networks of other commands. Responsive measures directed by combatant commanders will take precedence over responsive measures directed by Service INFOCON's. (Walker, 2000)

All combatant commands, Services and defense and combat support agencies are required to develop supplemental INFOCON procedures, specific to their command and consistent with the guidance in CM-510-99. These procedures may include criteria for establishing an INFOCON level and recommended or required actions. Appendix C provides the COMTHIRDFLT/USS CORONADO (AGF-11) INFOCON standard operating procedure as an example of implementation and reporting guidance for a specific unit.

F. KEYS TO SUCCESSFUL IMPLEMENTATION OF THE INFOCON SYSTEM

1. System Interface Description

It is critical that commands and agencies have a thorough understanding of the high-level system architecture of all networks within their domain. A thorough

understanding of an organization's system architectures will assist in understanding potential operational impacts if the INFOCON is changed. Architectures should accurately show interfaces between component parts and connectivity to systems outside the domain. Component parts can represent any entity (e.g. unit, department, directorate, etc.) that is considered part of the domain. Architectures provide a mechanism for understanding and managing complexity. A mechanism that can be used to represent architectures is the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework. The Framework provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating architectures. One product that can be used to show interfaces between systems or component parts is called the System Interface Description. An example of a generic System Interface Description from the C4ISR Architecture Working Group (AWG), C4ISR Architecture Framework Version 2.0 document is shown in Figure 1-1.

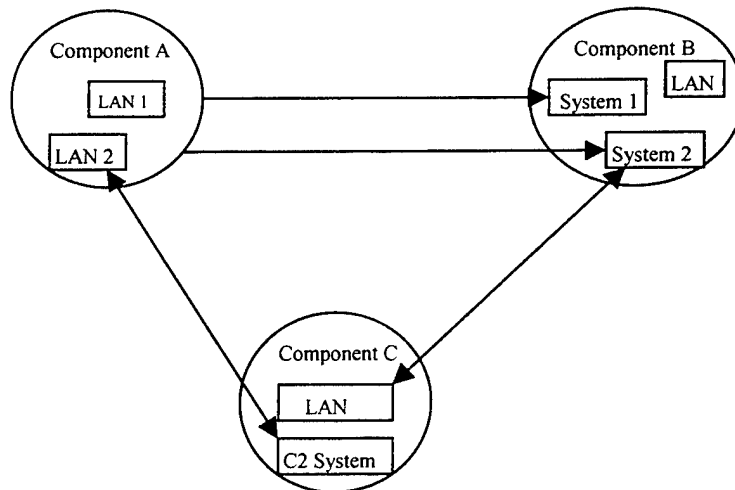


Figure 1-1. System Interface Description Example
(From C4ISR Architecture Framework, 1998)

2. System Communications Description

In addition to understanding the high level architecture and interfaces, network administrators should be aware of all network components, external connections to the networks, and all applications and databases that reside on the networks they are responsible for. This is the only way to accurately predict the affect of applying a particular countermeasure. For example, it is possible to fail in isolating compromised portions of an affected system because network administrators are not aware of all paths between nodes and may unintentionally leave key links operational, vulnerable to the hostile threat. By effeciently documenting the electronic communication path, workarounds and procedures to continue effective operations during INFOCON can be planned well in advance of an attack. A C4ISR product, the System Communication Description, can be used to display the network infrastructure at particular locations. An example of this diagram, taken from the C4ISR Architecture Framework document, is shown in Figure 1-2.

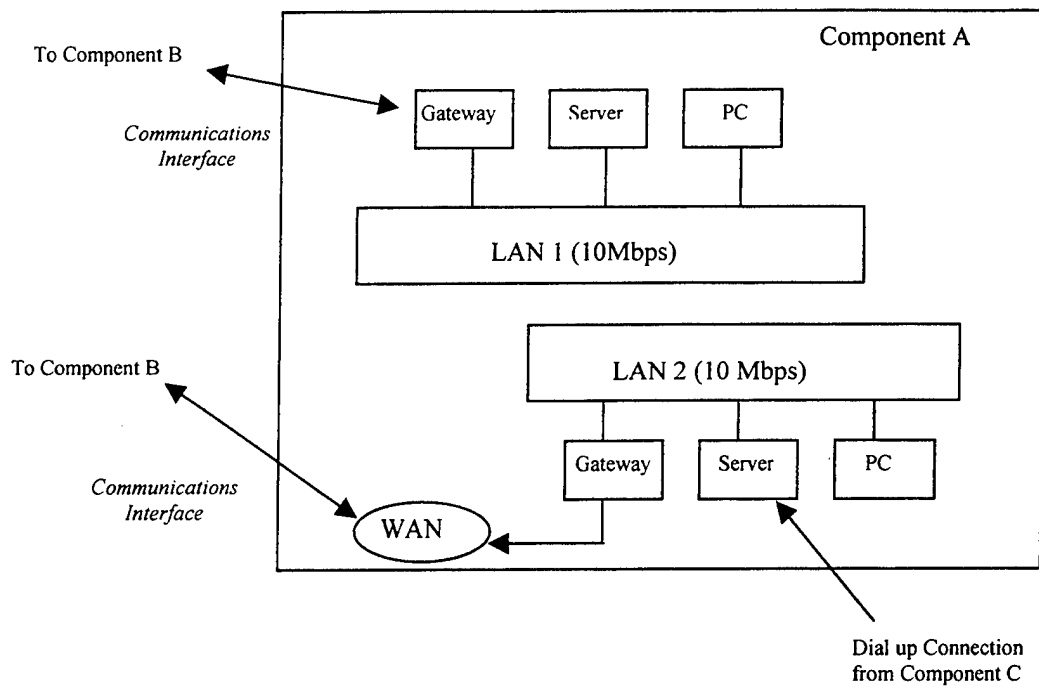


Figure 1-2. System Communication Description Example
(From C4ISR Architecture Framework, 1998)

3. Operational Node Connectivity Description

Once Networks are Defined, the support provided to military operations must be identified. In a recent interview with CDR (ret) Martin Greene, former Information Operations Officer on the COMTHIRDFLT staff and now INFOCON subject matter expert (SME) at the SPAWAR Information Operations Center of the Future (IOCOF) Lab in San Diego, he stated:

When the time comes to actually disconnect a system from a network, one must fully understand the affect this action will have on operations. Therefore, an operational view of architectures that include all command and control nodes must be captured. (Greene, 2000)

A simple C4ISR product that can be used in this effort is the Operational Node Connectivity Description. Figure 1-3 is an example of an Operational Node Connectivity

Description diagram taken from the C4ISR Architecture Framework document. This high-level diagram includes information exchanged between nodes or component parts and operational activities of each component part. Mr. Greene added:

Once system and operational views of networks are defined, the information should be integrated and displayed in a manner that makes it relatively easy to determine which operational activities would be affected if a network access were denied during a specific INFOCON. (Greene, 2000)

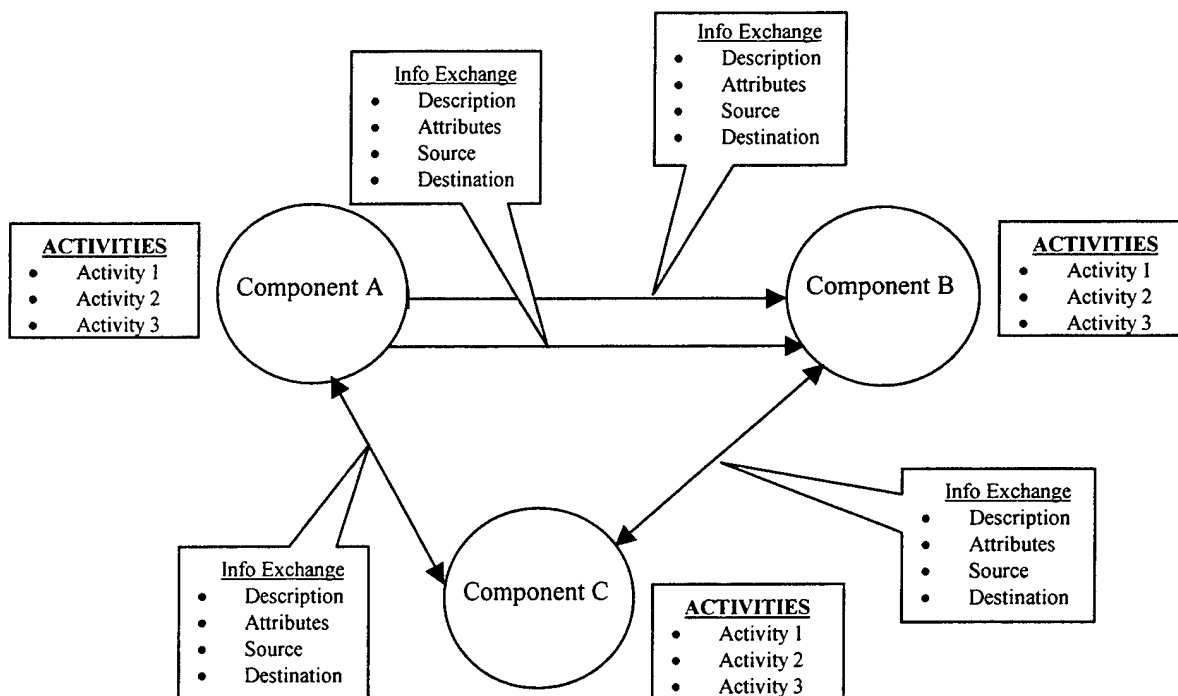


Figure 1-3. Operational Node Connectivity Description Example
(From C4ISR Architecture Framework, 1999)

In addition to fully understanding an organization's systems architecture as well as the command and control processes that integrate operational components, network administrators should understand their network bandwidth and throughput capabilities.

As stated in an article, Overview of Information Operations Condition (INFOCON), written for Cyber Sword by Ms. Regina Walker:

Knowledge of 'normal' throughput will help determine the effect of countermeasures. For instance, rerouting the normal flow of traffic on a network may result in increased use of bandwidth on available links and delay the arrival of messages at their destinations. Knowledge of network throughput may also help determine when an attack, such as denial of service, is underway because the network is saturated by extraneous message traffic. (Walker, 1999)

G. SUMMARY

The INFOCON system provides a standard and systematic approach to deal with the increasing problem of attacks on DoD networks. The five levels previously discussed indicate of the likelihood or severity of attack and provide guidance on what responsive measures should be implemented. While it is important that the appropriate INFOCON is declared, the ultimate success of the system depends upon thorough planning, rehearsal, execution, and daily vigilance.

INFOCON actions should be reviewed and tested often. This will help personnel understand their roles and responsibilities, determine the effect of responsive measures in an artificial environment, and detect problems in existing procedures. A recent experiment that the author participated in was conducted at the SPAWAR IOCOF with COMTHIRDFLT staff officers. The primary objective of the experiment was to investigate the relationship between military INFOCON's and their impact on warfighter's

ability to conduct operational command and control tasks. Chapter IV is a detailed review of this initial laboratory INFOCON experiment.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SPAWAR INFORMATION OPERATIONS COMMAND AND CONTROL (IO/C2) EXPERIMENT: THE IMPACT OF INFOCON LEVELS ON SIMULATED FLEET OPERATIONS

A. EXPERIMENT OVERVIEW

1. Operational Background

The Chairman of the Joint Chiefs of Staff (CJCS) Memorandum dated 10 March 1999 (CM-510-99) established the Information Operations Condition (INFOCON) system for the Department of Defense (DoD). The policy contained in this document focused specifically on defense against attacks on DoD computer networks. These computer network attacks are a subset of the broader discipline of Information Operations (IO). INFOCON actions were designed to heighten or reduce the defensive posture against computer network attacks, and to mitigate sustained damage to DoD computer infrastructures.

Given the CJCS Memorandum focus and the obvious need for data to support policy decisions, SPAWAR Systems Center (SSC) San Diego hosted an Information Operations/Information Assurance (IO/IA) symposium, which the author attended, in October 1999. During this event, several organizations agreed to form a partnership in support of an ambitious program of experiments designed to better understand the impact of the INFOCON's on Fleet command and control processes. The partners included SSC San Diego; SPAWAR, PMW-161; the Chief of Naval Operations (OPNAV), N-64; the

Navy Warfare Development Command (NWDC); and the Defense Advanced Research Projects Agency (DARPA).

Commander THIRD Fleet (C3F) staff officers participated in the initial IO C2 experiment. C3F routinely operates as both a Numbered Fleet Commander and Commander Joint Task Force (CJTF). During normal operations and exercises, the Battle Watch Captain (BWC) is the Commander's direct representative and the Battle Watch team interacts at an operational level with other C3F staff elements and external command staffs and watch teams.

As shown in the Figure 4-1, the SSC San Diego Information Operations Center of the Future (IOCOF) was configured as the USS CORONADO Joint Operations Center (JOC) for this IO C2 Experiment. Normal systems and communications paths were



Figure 4-1. IOCOF USS CORONADO JOC Configuration
(From SPAWAR IO C2 Experiment Brief, 2000)

available to watch standers to accomplish their mission with the exception of typical ship voice communications (e.g UHF/SHF/EHF). The SSC experiment planners decided to substitute Microsoft's NetMeeting in the experiment to enable a more robust reconstruction and more accurate watch stander evaluation. Tasks performed by the watch teams were identical to those tasks usually performed on watch in the JOC. This parallel structure between normal C3F staff operations and the experiment ensured realistic experimental fidelity. However, during a recent interview with Dr. George Seymour, IO C2 Experiment Senior Analyst, he stated:

This experiment evaluated a staff that is not concerned with the details of individual ship or other unit operations, positions, reports, logistics, etc. Instead, the operational commander is concerned with the aggregate performance of subordinate warfare commanders, who in turn rely on more detailed information to perform their mission. Therefore, the findings of this experiment should not be used to infer the impact of INFOCON's on other operational staffs outside the Battle Watch organization. Any assessment of INFOCON impacts on other staffs must be made independently. (Seymour, 2000)

The experiment used a naval scenario based in the South China Sea to provide a realistic operational setting for the Battle Watch participants. Pre-recorded Global Command and Control System Maritime (GCCS-M) track data provided a tactical picture for each watch. The scenario varied slightly from watch to watch to maintain operator interest and focus. Unlike a wargame that uses the scenario to drive a winning solution for the participants, this scenario served more as a backdrop, providing a context for routine Battle Watch actions. This allowed the experiment to focus on the variation

caused by the INFOCON level in effect for each watch. Each session represented a nominal 0400-0800 Battle Watch in an operational CJTF environment familiar to the participants. The emphasis was on conducting the watch rather than fighting the war as is the case in a typical wargame. Dr. Seymour explained that "the scenario events purposefully were not cumulative." (Seymour, 2000) That is, scenario events were independent for each watch period. The variable from watch to watch was the INFOCON level and attendant impacts on networks and tools available to the Battle Watch in the JOC.

2. Objective

The primary objective of this initial IO C2 experiment was to investigate the impact of military INFOCON's on the warfighter's ability to conduct operational C2 tasks. The key warfighting capability addressed was the ability of the staff to continue mission performance in a command and control center under network threats or attacks and the subsequent actions resulting from setting of INFOCON levels commensurate with the threat. Specific experiment capabilities were dependent on the particular function (e.g. J2, J3, J6, etc.) and the particular tasks associated with that function. Based on the experiment architecture and scenarios, the objectives as indicated in the SPAWAR IA C2 Experiment Test Plan were to determine the following:

- What impact on the warfighter's C2 capability does a particular INFOCON have?
- What tasks cannot be completed as a result of a particular INFOCON setting?
- Is there an increase in time to complete a specific task?

- What workarounds do warfighter's employ to enable them to carry out their mission?

A secondary objective of the experiment was to create a realistic warfighting environment and foster a contextual awareness among the participants about INFOCON implications. We were tasked to quantify capabilities lost, verify C2 and Situational Awareness (SA) impact due to INFOCON level, and then identify workarounds that might be used during actual INFOCON situations. These objectives implied the need for quantitative measures for "impact" and "SA", as well as structured open-ended questions about related topics.

3. Scientific Background

a. Workload Measurements

According to H.G. Hart and L.E. Staveland, "the typical assumption in cognitive research is that workload is a hypothetical construct that represents the cost incurred by a human operator to achieve a particular level of performance." (Hart & Staveland, 1988) In preparing the plan to conduct this experiment, Dr. George Seymour wrote that "this common assumption implies that work is both more human-centered than task-centered, and that the subjective experience of work will be different for different people concerning the same task." (Seymour, 2000) For these reasons, the decision was made by the experiment planning team to use the NASA Task Load Index (TLX) as a measure of warfighter impact. In this model of work, workload is not an inherent

property of work but rather an interaction between the work requirement and the perception of the worker.

The NASA Task Load Index is a thoroughly studied, multi-dimensional, subjective rating procedure that affords an overall workload score based on the weighted average of six sub-scale ratings: (1) Mental Demands, (2) Physical Demands, (3) Temporal Demands, (4) Performance, (5) Effort, and (6) Frustration. This rating system was used to determine the workload that subjects felt they were exposed to during the course of the experiment. The NASA TLX procedure relates workload demands imposed on the subjects and the interaction of the subject to the task. Mental, physical, and temporal demands relate to the demands imposed on the participant from exterior sources, while the other three, performance, effort, and frustration, relate to the interaction of the participant with the task they are performing. In addition to the six scale score, a weighted measure of task load can be calculated based on the sub-scales. Definitions for each of the six sub-scales are shown in Appendix D.

b. Situational Awareness Measurements

Another critical component of this research effort involved Situational Awareness (SA). According to Dr. W.G Kemple and Professor S. Hutchins from the Naval Postgraduate School (Evaluating Human Performance in Command and Control Environments), "SA refers to the decision maker's moment-by-moment ability to monitor and understand the state of the complex system and its environment. Generally speaking, the concept of SA refers to the mental process of knowing what is going on at any point

and time in the surrounding environment." (Kemple & Hutchins, 1999) Traditionally, human factor researchers have focused on awareness as explicit knowledge that is created through an interaction between a subject and the environment. SA is important in military decision making for several reasons. It provides the foundation for subsequent decision making and action selection in complex, dynamic environments. When emergencies arise, the completeness and accuracy of the decision maker's SA are critical to the ability to make decisions, revise plans, and manage the system. Finally, maintaining accurate SA is critical for conducting coordinated operations involving shared command and control resources.

A Framework of Awareness for Small Groups in Shared Workspace, a Technical Report by C. Gutwin and S. Greenberg, identified four fundamental characteristics that distinguish awareness from other kinds of knowing. Their discussion of the four characteristics follows. (Gutwin & Greenberg, 1999)

- Awareness is knowledge about the state of some environment, a setting bounded in time and space. For example, the environment might be the airspace that an air traffic controller is responsible for, and his/her knowledge might include aircraft headings, altitudes, and separation, and whether these factors imply a safe or unsafe situation.
- Environments change over time so awareness is knowledge that must be maintained and kept up-to-date. Environments may change at different rates, but in all cases a person must continually gather new information and update what they already know.
- People interact with the environment, and the maintenance of awareness is accomplished through this interaction. People gather information from the environment through sensory perception, and actively explore their surroundings based on information they pick up.

- Awareness is almost always part of some other activity. That is, maintaining awareness is rarely the primary goal of the activity. The goal is to complete some task in the environment.

Despite its almost universal appeal in the military, there is little consensus about the assessment method or measurement of SA. For that reason, the experiment planning team decided to let each of the participants, senior naval officers with extensive tactical experience in command center functions, estimate his own awareness level, but under structured conditions. At the end of each watch, each participant was asked to complete a Situational Awareness form to provide this estimate. A scale anchored between 1 (poor) and 10 (outstanding) was used and that signified each participants SA at that point in time. As mentioned above, the measure was obtained at the end of each watch before any group discussion or subject matter expert (SME) feedback. At the same time, each participant was asked to identify his C2 capability using the same anchored scale. In addition to the participants providing their own assessment of SA at the end of each watch, two SME facilitators provided an assessment of SA for each participant based on interactions with the participants during and at the end of each watch. The SME's used the same anchored scale from 1 to 10.

B. EXPERIMENT DESIGN

1. Experiment Architecture

"Defining the test bed C4I architecture was a compromise between credibility, complexity and cost effectiveness. It was important that the results of the experiment

stand up to both technical scrutiny and, more importantly, to operator scrutiny." (Seymour, 2000) Although the test bed infrastructure did not permit the installation of a complete Command Ship C4I suite, it did replicate a representative cross section of the fielded computers and communications suites on the C3F Command ship. This permitted a reasonably large number of Battle Watch personnel to operate in the lab for the scenario periods as if they were embarked on an actual Navy command ship. The test bed, for all practical purposes, was a representative Navy command ship operational space, populated with operational systems and driven by realistic data. Using this environment facilitated the immersion of operators into an experience that both supports the collection of experimental data and serves as the basis for the development of future Information Operations (I/O) doctrine and tactics.

In most cases test bed servers were normal PCs or UNIX workstations that represented the hardware in the Fleet. The focus was to run the fielded server software, or a more cost-effective solution as appropriate, to achieve representative functionality. Figure 4-2 illustrates the location and tools available to each experiment participant. Figure 4-3 provides a diagram of the experimental Joint Operations Center big screen displays configured for this experiment.

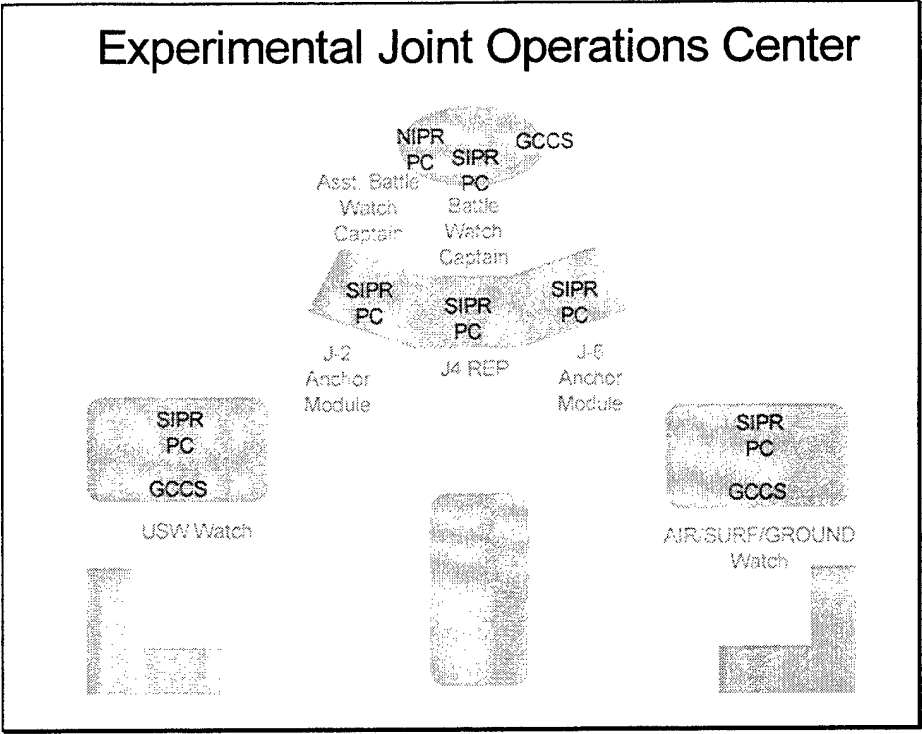


Figure 4-2. Experimental Joint Operations Center (JOC) Configuration
(From IO C2 Experiment Test Plan. 2000)

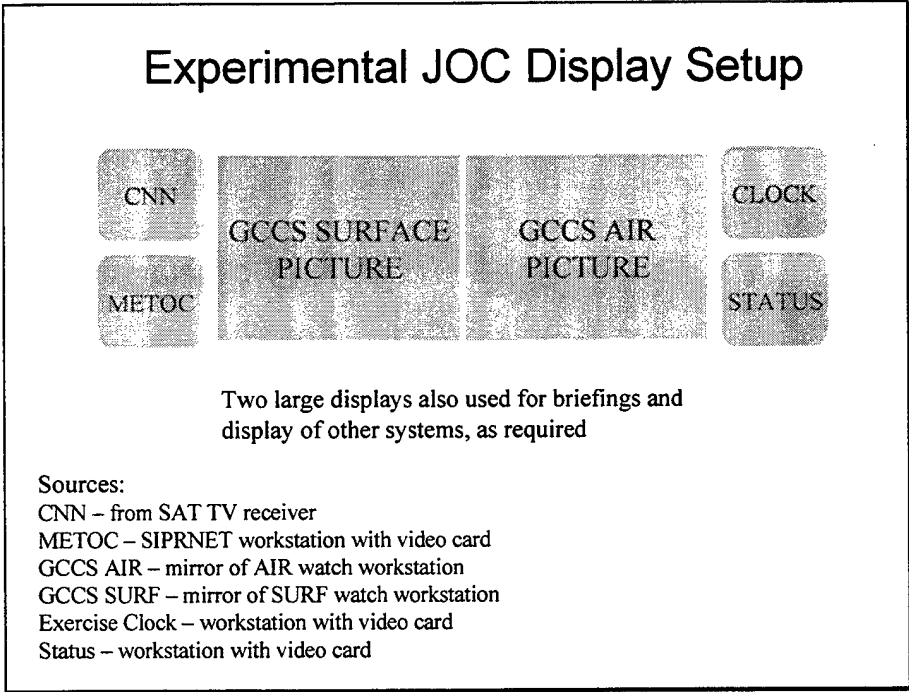


Figure 4-3. Experimental Joint Operations Center Display Configuration
(From IO C2 Experiment Test Plan, 2000)

a. *Experimental UNCLASSIFIED Network*

The experimental UNCLASSIFIED network configuration capabilities are listed below and illustrated in Figure 4-4. This information was provided by the SPAWAR IOCOF experiment support personnel.

- SailorNet workstations
 - Used for sailor unclassified email and web surfing
 - Simulated Legal, Public Affairs, Medical unclassified systems
 - Personal Computer (PC) running Windows NT Workstation
- Assistant Battle Watch Captain workstation
 - Used of unclassified email and web surfing
- Web proxy server
 - Provided network address translation and access to the Internet for live network connection

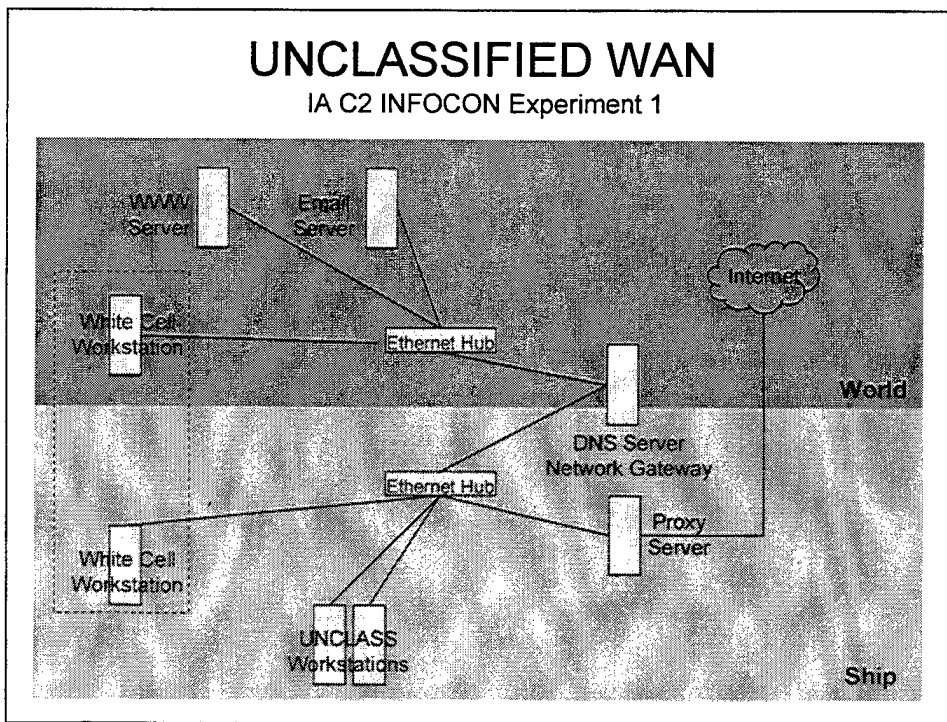


Figure 4-4. Experimental Unclassified Network Configuration
(From IO C2 Experiment Test Plan, 2000)

b. Experimental SECRET Network

The experimental SECRET network configuration capabilities are listed below and illustrated in Figure 4-5. This information was provided by the SPAWAR IOCOF experiment support personnel.

- Exchange Server
 - PC running Windows NT (WinNT) Server 4.0 and Microsoft Exchange
- File Server
 - PC running WinNT Server 4.0
- NT Primary Domain Controller
 - PC running WinNT 4.0
- Global Command and Control System Maritime (GCCS-M) Servers
 - JOTS-1, JOTS-14, JOTS-19
 - HP UNIX system
- Web Server
- PC's (6) for JOC BWC and anchor modules
 - WinNT Workstation running Microsoft Office, Microsoft Outlook, web browser, file server access, C2PC or equivalent functionality, shared log system, Microsoft NetMeeting to simulate voice communications
- GCCS-M workstations (3)
- CTAPS Workstation (1)
- Proxy Server
 - Provided network address translation and access to SIPRNET for live network connection
 - Simulated SIPRNET WAN problems and implemented INFOCON SIPRNET disconnect

- PC running WinNT 4.0 and Microsoft Proxy Server
- Repeat System
 - Used to inject pre-recorded message traffic into GCCS-M system to simulate operational data flow
 - PC running WinNT 4.0

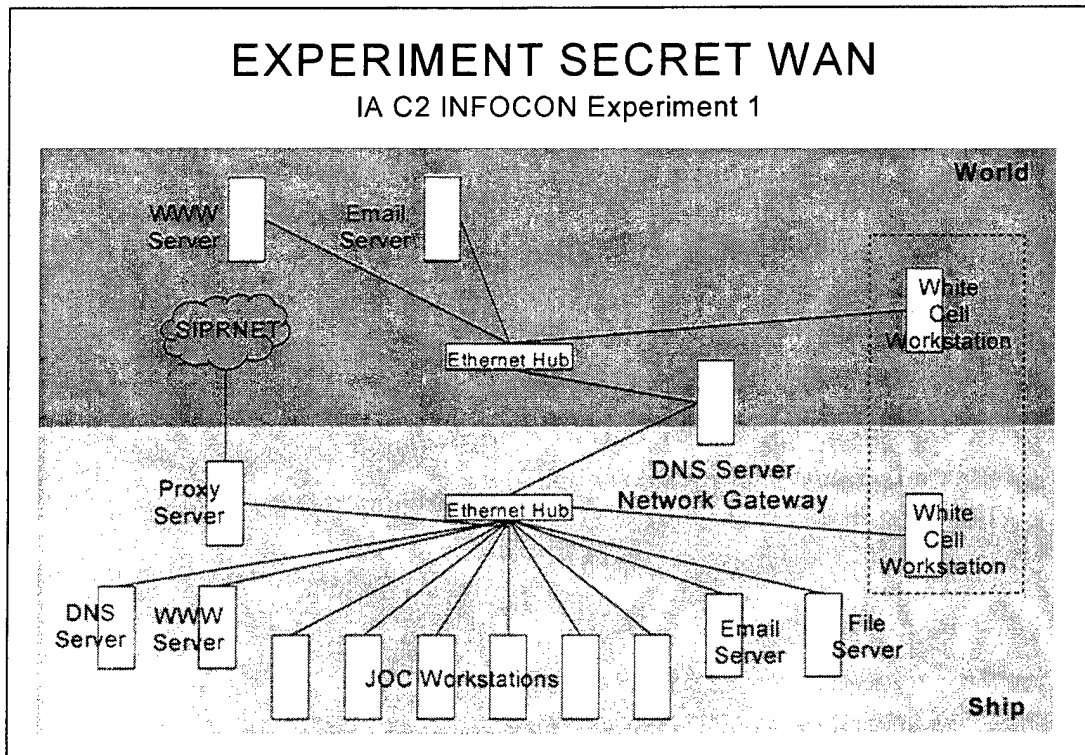


Figure 4-5. Experimental SECRET Network Configuration
(From IO C2 Experiment Test Plan, 2000)

2. Experiment Participants

a. Test Subjects

Seven test subjects, one at each computer workstation, participated in this realistic simulation of the C3F Joint Operations Center. The participants were senior naval officers who were fully qualified and experienced with the duties in the JOC. "The

officers who served as participants had a combined total military experience of 126 years, and their mean age was 39.3 years." (Seymour, 2000) The participant's professional disciplines consisted of three Surface Warfare Officers (SWO), two Cryptology Officers, one Intelligence Officer, and one Limited Duty Officer (LDO) specializing in cryptology. These officers typically worked together as part of a team on the C3F Flagship.

b. Observers

Four independent observers monitored the experiment and logged subjective comments during each watch. The author participated in this capacity throughout the effort. Each observer was assigned to monitor two adjacent workstations of the experiment, and distribute and collect data forms during each phase of the experiment. Each observer underwent an hour of training in group session to familiarize each with the scenarios for each watch, as well as the data collection instruments and timing.

c. Subject Matter Experts (SME's)

Two SME's acted as experiment facilitators. Both SME's had extensive experience as naval officers in the skills and requirements for JOC watch standers. The facilitators provided the watch team with the typical information given to a JOC watch team as "pass down" before assuming the watch. The information included daily brief guidance and the current events that were being monitored in the JOC. In addition, the SME's were responsible for assessing the watch team situational awareness at the conclusion of each watch.

3. Role-Based Functionality

The Joint Operations Center (JOC) serves as the focal point for senior decision-makers aboard Flagships like the USS CORONADO. However, the majority of the C4I functionality and operations for C3F are carried out in other operational spaces. For example operations efforts are also conducted in the Joint C4I Coordination Center (JCCC), Joint Air Operations Center (JAOC), Joint Intelligence Support Element (JISE), and the Tactical Flag Command Center (TFCC). Interfaces between the JOC and these other supporting organizations are primarily via voice communications, shared logs and email. The experimental architecture provided a simulated interaction with these other organizations via email, message traffic, shared logs and GCCS track updates. The architecture supported positions modeled from the C3F JOC. The experiment watch positions with respective network connectivity capabilities is shown in Table 4-1.

Table 4-1. IO C2 Experiment Role-Based Functionality

Test Subject	Secret PC	Unclass PC	MS Office	MS Outlook	Web Browser	MS NetMeeting	GCCS-M
Battle Watch Captain	X		X	X	X	X	X
Assistant Battle Watch Captain		X		X	X	X	
Air Watch	X		X	X	X	X	X
USW Watch	X		X	X	X	X	X
J2 Anchor Module	X		X	X	X	X	X
J6 Anchor Module	X		X	X	X	X	X
J4 Anchor Module	X	X	X	X	X	X	X

4. Variables

The independent variable for the experiment, INFOCON level, was defined at the start of each Watch, and operationalized by manipulating or reducing networked communication capability in increasing steps in accordance with the C3F INFOCON Instruction (see Appendix C). Similar to the Fleet and joint operational counterpart, the experiment INFOCON levels range from Normal through Delta, and were varied one level (Watch) at a time. Its imposition was explicit to the participants at the start of each watch and remained constant throughout that watch.

Four dependent variables were measured at the end of each watch. These included: Workload Impact, Situational Awareness, C2 Capability, and Time Delta as measured by asking the test subjects to estimate how much longer it took each to complete their task under each INFOCON condition when compared to INFOCON Normal.

5. Procedure

Five different watches, each lasting approximately three hours and corresponding to the five INFOCON levels, were conducted. Appendix F shows the experimental task and procedure flow for each of the five watches, as well as their data collection points. Watch One (INFOCON Normal) was used as a training exercise and served mainly as an introduction to the subsequent four watches. Watches two through five represented INFOCON levels Alpha, Bravo, Charlie, and Delta, in order of presentation and where an increasingly restrictive network posture was implemented.

The NASA Task Load Index (TLX) is a subjective rating procedure that was used to measure each participant's workload assessment during the varying INFOCON levels. The NASA TLX is a two-part assessment process consisting of both task weightings and task ratings. Figure 4-6 and Figure 4-7 are the TLX Factoring forms that were used to collect the weightings from each test subject after the INFOCON Normal watch.

Workload Instrumentation

TLX Factoring: Part A

First, before we start the experiment, think about the work you typically perform at your computer workstation during normal operational conditions at sea. Then, using the TLX Work Scale Definitions that you just read, think about which of the following aspects of your work are the **most important** contributors to your workload during a typical operational day.

MENTAL DEMAND	= MD
PHYSICAL DEMAND	= PD
TEMPORAL DEMAND	= TD
EFFORT	= EF
PERFORMANCE	= O P
FRUSTRATION LEVEL	= FR

With that in mind, and using the two letter codes above, choose the one letter pair from each pairing below that is most important to your workload (workload centrality). In other words, if the physical demand (PD) of your typical workload is more important each day than the mental demand (MD), circle the PD in the upper left pairing below. Continue to make your choices for all 15 pairings.

PD / MD	TD / PD	TD / FR
TD / MD	OP / PD	TD / EF
OP / MD	FR / PD	OP / FR
FR / MD	EF / PD	OP / EF
EF / MD	TD / OP	EF / FR

Date/Time: _____

Workstation: _____

Figure 4-6. TLX Task Weighting Instrument - Part A

Workload Instrumentation

TLX Factoring: Part B

Next, think about the work you typically perform at your computer workstation during normal operational conditions at sea. Then, using the TLI Work Scale Definitions that you read previously, think about which of the following aspects of your workload **change the most** during a typical operational day.

MENTAL DEMAND	= MD
PHYSICAL DEMAND	= PD
TEMPORAL DEMAND	= TD
EFFORT	= EF
PERFORMANCE	= OP
FRUSTRATION LEVEL	= FR

With that in mind, and using the two letter codes above, choose the one letter pair from each pairing below that changes the most (workload variation). In other words, if the physical demand (PD) of your typical work varies more each day than the mental demand (MD), circle the PD in the upper left pairing below. Continue to make your choices for all 15 pairings.

PD / MD	TD / PD	TD / FR
TD / MD	OP / PD	TD / EF
OP / MD	FR / PD	OP / FR
FR / MD	EF / PD	OP / EF
EF / MD	TD / OP	EF / FR

Date/Time: _____

Workstation: _____

Figure 4-7. TLX Task Weighting Instrument - Part B

The first part of the TLX process required participants to make a choice between each pair combination among the six sub-scales shown in the figures above. This was accomplished after the first INFOCON session (Normal). Each test subject was asked to consider which "aspects of your work were the most important contributors to your workload." (Hart & Staveland, 1988) then fill out the forms above. This helped obtain a numerical rating for each scale that reflected the magnitude of that workload factor in a given task.

The second part of the process required each individual to evaluate the contribution of each workload factor to the total workload of a specific task. The weighting score provided an indication of the importance of each dimension, relative to the other dimension to the overall task. "The weighting accounts for two potential sources of differences between raters: differences in workload definition within a task and differences in the sources of workload between tasks." (Hart & Staveland, 1988) Figure 4-8 shows the TLX rating scale forms that each participant completed at the conclusion of each watch.

6. Tasks

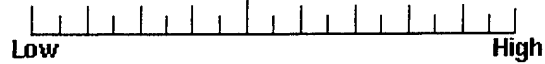
Each of the five watches, corresponding to the five INFOCON levels, consisted of an approximately three hour scenario-driven set of events typically found on Navy command ships. Appendix F, IA C2 IOCOF experiments design & data collection flow diagram, illustrates the event time sequence for each watch. Each watch commenced with

Workload Instrumentation

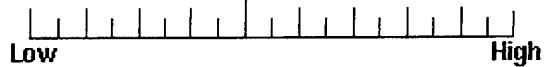
TLX Rating Scales

Use the following six scales to evaluate [1=(LOW) to 10 =(HIGH)] the work you have been doing during the past few hours. Place a check mark (✓) on each line below, and also write the corresponding whole number (1 through 10) to the right of each scale.

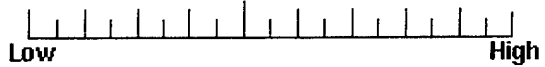
MENTAL DEMAND



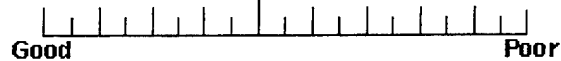
PHYSICAL DEMAND



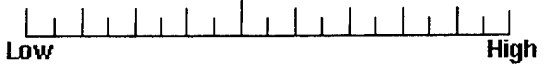
TEMPORAL DEMAND



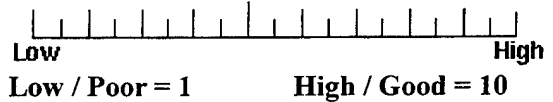
PERFORMANCE



EFFORT



FRUSTRATION



At this time, what is your most important task: _____

Using a scale from 1 (poor) to 10 (excellent), what is your current task-related Situation Awareness level: _____

At this time, what is your estimate of the amount of **INCREASED** time that it will take you to complete your task for this scenario (range from zero to hrs. or days):

Date: _____ Time: _____
INFOCON Level: _____ Workstation: _____

Figure 4-8. TLX Rating Scales Form

a situation brief from the off-going watch (Subject Matter Expert) to set the stage/course of action for the test subjects. The command and control systems were configured to match the experimental threat condition/INFOCON level and the participants executed a specific set of tasks based on the operational requirements of the scenario.

To ensure adequate contextual realism for the experiment, the test subjects and SME's were responsible for completing three distinct measurement tasks during each watch that provided data used in the analysis effort. Metrics for this experiment were designed and instituted by Dr. George Seymour from SSC San Diego. The following provides an excerpt from Dr. Seymour's experiment write up that discusses the approach used to help measure situational awareness for this experiment. (Seymour, 2000)

1. Commander's Daily Brief Preparation Support. The military watch selected for this experiment (0400-0800) corresponds to the period when a briefer would query the Battle Watch for current information to support the preparation of the daily brief. The test subjects were tasked to complete a daily brief information matrix that provided a measure of the watch's ability to ascertain what had occurred during the watch in all areas of concern to the JTF Commander. This information was reported by the JOC approximately two-thirds of the way through each Watch. The SME's used this information to estimate the overall situational awareness of each Watch using a scale from 1 (poor) to 10 (outstanding).
2. Commander's Daily Intentions Message Support. Each test subject was tasked to provide inputs to the Commander's daily intentions message at the end of each Watch. By supplying this information, the Battle Watch team demonstrated its specific understanding of the impact on future operations and thus offered a recommended priority the Commander could take in order to respond effectively to mission requirements. The SME's used this information in their estimate of the overall situational awareness of each Watch, again a scale of 1 to 10.
3. Off-going Watch Pass Down. At the conclusion of each watch period the test subjects provided an off-going brief to the 'relieving' watch team (SME's). This brief verified each participant's situational awareness at the conclusion of that watch. This pass down mimics a real watch-standing requirement, and thus afforded the facilitators a chance to extract and refine lessons learned from each watch. The

SME's used this information to further evaluate each participant's situational awareness during each watch, using a scale from 1 (poor) to 10 (outstanding).

Situational Awareness was measured in three ways. First, by asking each test subject to provide an estimate of his own SA at the end of each watch, second, by having the SME facilitators estimate the SA of each subject at the end of each watch, and third by having the SME's provide a single estimate of the watch team overall SA at the end of each watch. These scales ranged from 1 (poor) to 10 (outstanding).

Prior to the commencing the experiment, test subjects were provided an adequate period of training time to become familiar with the experimental tools and task expectations. After test subjects were familiar with their respective tasks, a set of weightings was obtained which described how each subject related to his specific task (refer to Figures 4-6 and 4-7). Dr Seymour stated that:

Prior to obtaining the workload scores (ratings) at the end of each watch, each participant provided work factor weightings that identified the relative weight of each work dimension to the overall task. These weightings explicitly acknowledge that work is a combination of external influences and internal perceptions, and thus likely to differ from person to person." (Seymour, 2000)

The six TLX scales, taken two at a time required fifteen choices by each test subject. After the choices, each subject assigned a weighting factor ranging from 0 to 5 for each of the six scales. The weighting factors were used to weight the participant's workload scores that were collected at the end of each watch. Each score was multiplied by its corresponding weighting factor and the results summed. Test participant's completed the workload score form at the completion of each of the five watches.

C. RESULTS

Measures for Workload Impact, Situational Awareness, C2 Capability, and Time Impact data were collected at the end of each Watch using the forms described in the previous section. These data were analyzed separately and are reported below.

1. Workload Impact

Prior to obtaining the workload scores (ratings) at the end of each watch, each test subject completed several TLX workload factoring forms that provided work factor weightings and identified that subject's relative weight of each scale to the overall task (refer to Figures 4-6 and 4-7). Subject's weightings were multiplied by their respective workload rating for each scale for each watch. These products were summed across scales and participants within watches and provide the basic workload data points for this experiment. Figure 4-9 provides the mean workload values as assessed by the NASA TLX, for all five Watches. "These data represent the weighted sums across seven participants within each INFOCON level. The mean workload scores ranged from a low at INFOCON BRAVO to its highest level at NORMAL." (Seymour, 2000) It should be observed that the workload during INFOCON Alpha is higher than INFOCON Bravo. However, this could be attributed to experimental learning. The test participants may not have been thoroughly familiar with the experimental tools during INFOCON Alpha and adjusted during the subsequent experiment watches.

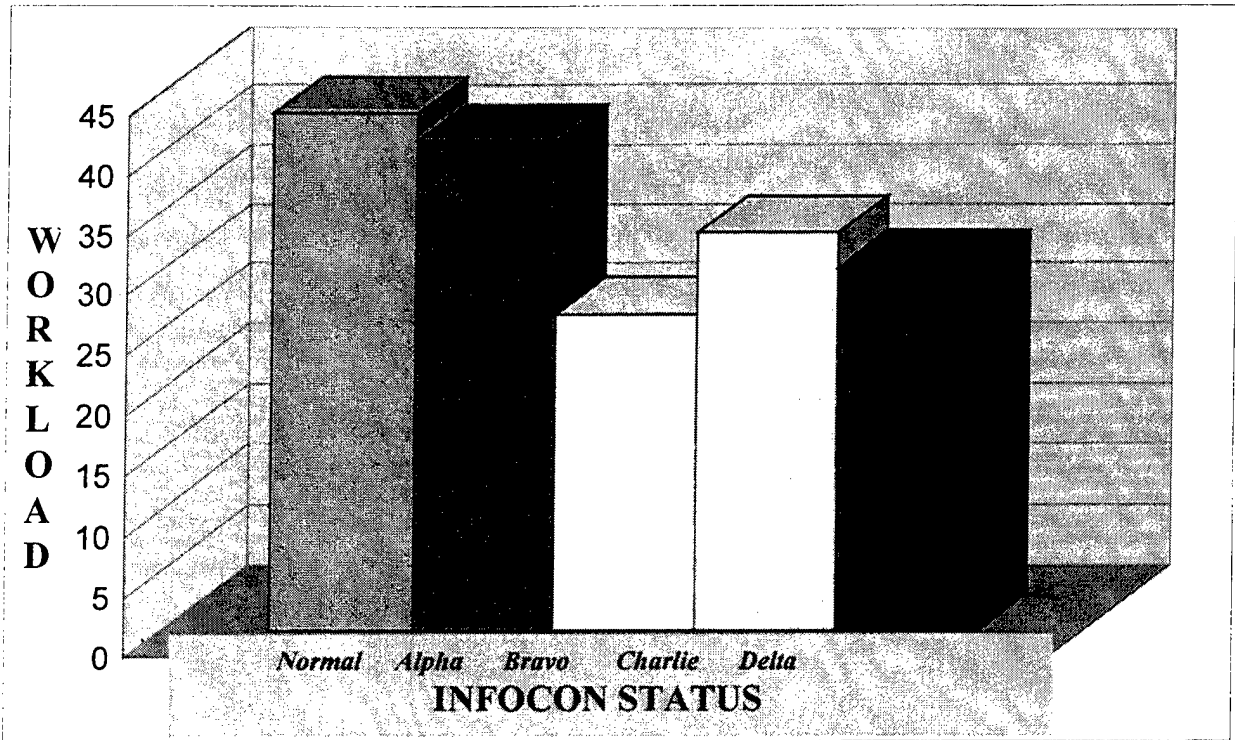


Figure 4-9. Impact of Increasing INFOCON Levels on JOC Workload
(From SPAWAR IO C2 Brief, 2000)

2. Situational Awareness

Situational Awareness (SA) and command and control (C2) were assessed by asking the participants to provide their own estimates at the end of each watch, before any group discussion. Hence, these remain relatively independent measures, free from group bias. Each participant provided a number between 1 (poor) and 10 (outstanding). The mean scores for both SA and C2 for each watch are shown in Figure 4-10. This figure indicates that the JOC situational awareness (SA), as well as the teams C2 capability, increased steadily through INFOCON Bravo, then it decreased for INFOCON Charlie, and further decreased during INFOCON Delta.

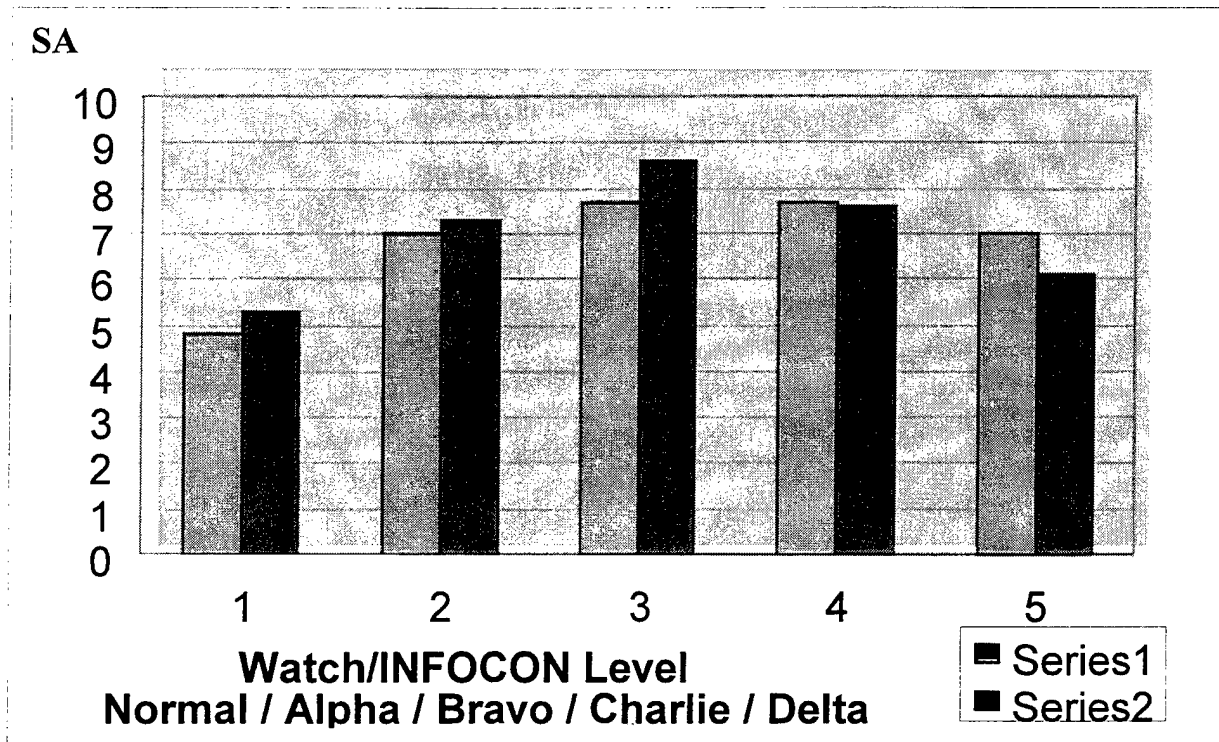


Figure 4-10. Impact of Increasing INFOCON Levels on Situational Awareness (Series 1) and C2 Capability (Series 2) (From SPAWAR IO C2 Brief, 2000)

3. Time Delta

Decision makers (e.g. Commanders, policy makers, network administrators, etc.) share an equal interest in knowing if and how much increased time will be necessary to complete operational or mission-related tasks when networked resources are diminished or curtailed. That is especially true for tactical C2 tasks. Therefore, each participant was asked to track the additional time it took to complete similar tasks under various INFOCON level implementations. The comparison point was INFOCON Normal. Figure 4-11 shows the average of the participant's time estimates to complete tasks at each INFOCON level. Figure 4-11 also shows that the least impact in terms of increased

operational time to complete the mission was during INFOCON Bravo, whereas the most additional time reported to complete the JOC mission-related tasks was during INFOCON Delta. These results correlate to the Workload and Situational Awareness results highlighted above.

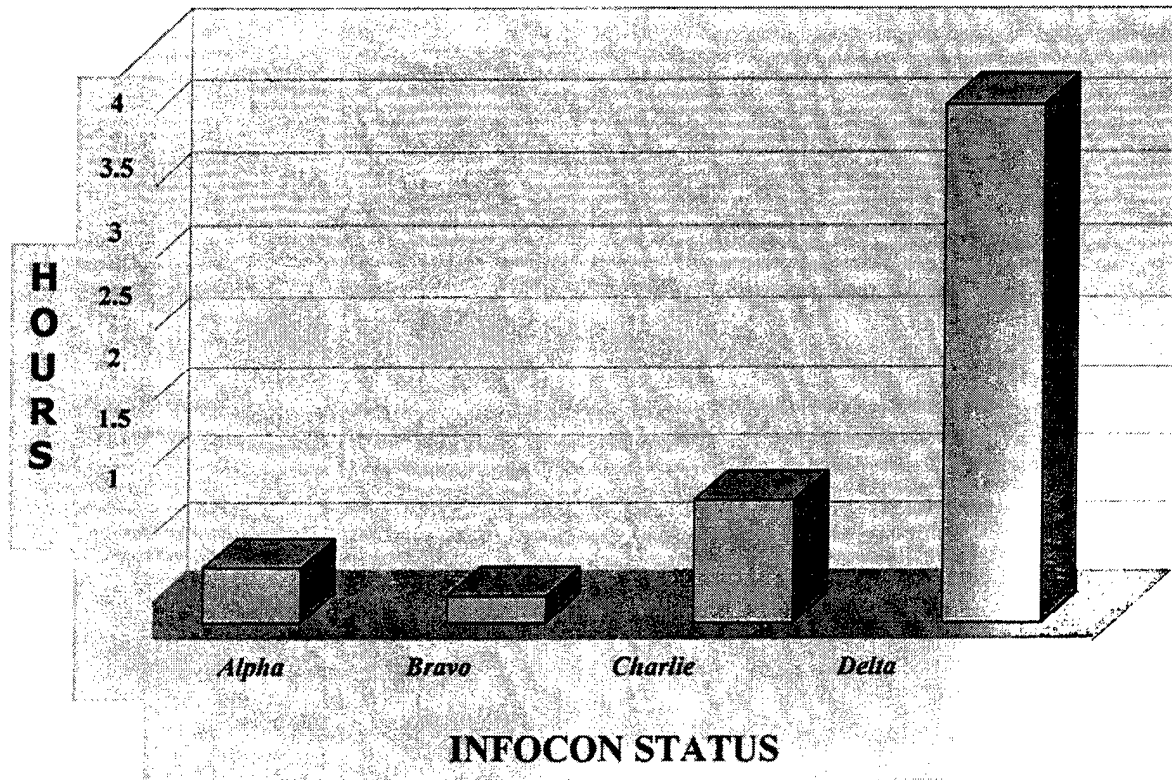


Figure 4-11. Participant Estimates of Increased Time to Complete Tasks
(From SPAWAR IO C2 Brief, 2000)

4. Lessons Learned

Participant's provided subjective comments that were reviewed after the experiment. Because of the participant's military experience and seniority, their comments and perspective provided a valuable source of information about the impact of INFOCON's on tactical C2 operations. From these comments we learned that:

- INFOCON's will impact their C2 work

- Impact is dependent on the specific C2 task
- Formal IA training is practically negligible
- Until INFOCON Charlie or Delta, C2 functions can be supported

In addition, from conversations with the experiment participant's, subject matter experts, and observers, it is clear that any impact of INFOCON status will not be uniform across naval environments.

Apparently, from these findings, many tactical C2 tasks can be performed at INFOCON levels Alpha and Bravo with no serious consequences. At the same time, depending on how long any INFOCON lasts, important ship functions, including logistics, medical, and email connectivity for the crew, would suffer at INFOCON Alpha or Bravo. Clearly, additional research is required to address these issues. (Seymour, 2000)

Both additional experimental (laboratory) and new operational exercise and survey research is needed to explore the questions that surfaced, yet remained unanswered, from this effort.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INFOCON FIELD EXPERIMENTATION METHODOLOGY

Sufficient training, including realistic exercises that simulate peacetime and wartime stresses, shall be conducted to ensure that commanders of U.S. Armed Forces are well-informed about trade-offs among affecting, exploiting, and destroying adversary information systems, as well as the varying capabilities and vulnerabilities of DoD information systems. (Joint Doctrine for Information Operations, 1998)

A. FIELD SETTING OVERVIEW

1. Exercises Versus Experiments

Exercises and experiments are both intimately tied to doctrine, but they have fundamentally different purposes. The purpose of an exercise is to train units to fight in accordance with established military doctrine and existing procedures. That is, a unit engages in exercises in order to develop and maintain the ability to apply doctrinal principles to prevail in war. They maintain readiness through training. An exercise is typically designed so the units being trained will succeed and is conducted with certain training goals in mind. According to the Naval Research Council study, Realizing the Potential of C4I, "The purpose of an experiment is to explore alternative doctrine, operational concepts, and tactics that are enabled by new technologies or required by new situations." (NRC, 1998) That is, new technologies, procedures, or situations like INFOCON implementations may call for different ways of conducting operations under certain conditions. However, without actual operational experience in using new technologies or procedures, experiments are needed that will provide a basis for making

informed decisions and ultimately for identifying doctrinal changes that will support today's warfighter.

2. Laboratory Experiment to Operational Environment

Any type of experimentation, to be successful, requires a great deal of planning for capture of data and subsequent analyses. Both must be linked to a set of learning objectives. There is a progression of types of experiments, from those that are simple to plan to those that tax the most ingenious minds. (Schacher and Gallup, 2000)

If one moves from the laboratory to the operational environment, experimentation becomes more difficult. This is due in a large part to lack of control over the environment. The term control is used in several different senses in experimental design. One sense refers to the ability to control the situation in which an experiment is being conducted so as to keep out extraneous factors that could impact the outcome of the experiment and lead to incorrect causal inference. Laboratory experiments offer a better opportunity to implement this type of control to obtain a desired result. However, because control over independent variables in field experiment design are difficult to implement, researchers must anticipate causal inference under operational conditions.

If humans are part of the experiment, or if environmental conditions are changing, control is very complicated and methods to capture the human-in-the-loop interactions within the environment are difficult to implement. "One has to develop means for accounting for the variability of human behavior, or set up environment controls within which human interactions can be investigated." (Schacher and Gallup, 2000) A researchers central concern prior to collecting data for analyses must be a complete

understanding of the operational environment. In addition, repeatability, the ability to obtain like results from multiple experiment runs, is very difficult in field environmental experiments. Hence, obtaining similar results to answer the overall objectives of the experiment multiple times may mean waiting for the right conditions to occur.

B. MODULAR COMMAND AND CONTROL EVALUATION SYSTEM

The Modular Command and Control Evaluation System (MCES) is a general C3 evaluation model developed by several Military Operations Research Society (MORS) command and control experts. This approach provides a series of seven modules conducted in an iterative process to evaluate alternative C3 systems and architectures. The seven modules include problem formulation, system bounding, process identification, measurement identification, data collection, and data aggregation. The author chose to use the MCES methodology as the framework for discussing an INFOCON experiment in a field setting. Figure 5-1 illustrates the MCES structure.

When expanding the INFOCON laboratory experiment to a field environment, the MCES methodology will help planners and analysts develop an experimental design that will ultimately capture the data required to support the analysis of the relevant experimental questions. The MCES presents a method to attack difficult concepts in a standardized manner. "Ultimately the MCES can be thought of as two processes, a managerial system which serves as a guide to specifying the problem to be analyzed, and an analytic system which serves as a guide to the analysis process itself." (Sweet, 1986)

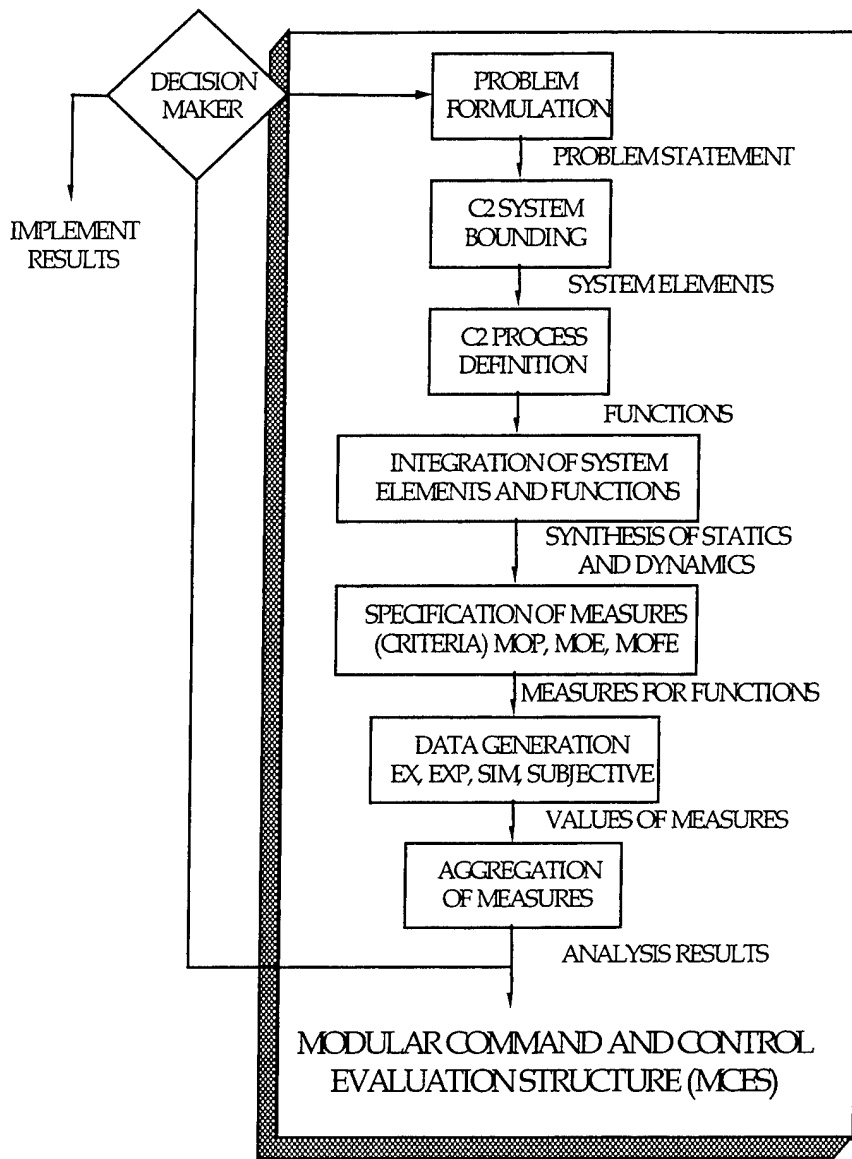


Figure 5-1. Modular Command and Control Evaluation Structure (MCES)
 (From MCES Methodology, 1986)

C. INFOCON PROBLEM FORMULATION

The MCES process begins by identifying the objective of a particular application like an INFOCON implementation, which leads to the first module, problem formulation. For example, if a commander wants to know the C2 implications of an INFOCON implementation on his Battle Watch Staff or his logistics organization, then that

experimental requirement must be articulated. The INFOCON operational and deployment concepts, environmental factors, scenarios, assumptions and threats must be made explicit to clearly formulate the problem. In this module, both the appropriate mission and scenario within the context of the experiment are made explicit. During the IO C2 laboratory experiment described in Chapter IV, the problem articulated was to identify the Battle Watch Staff capabilities and time lost due to INFOCON implementations and to document C2 and situational awareness impacts due to those specific implementations. Similarly, this problem could be expanded to an operational environment. Hence, the data that was collected and analyzed in the laboratory environment can serve as the baseline for the anticipated results in a field setting.

In the implementation of this step, the answers to several questions, which encompass an early review of the seven MCES modules, may provide guidance for developing the experiment plan. Some example questions that should be considered during the INFOCON problem formulation phase are:

- Who are the decision maker(s), and how are decisions made under normal conditions?
- What mission area(s) are involved?
- What are the basic assumptions of the problem?
- What threat and scenarios are appropriate and available?
- What level (system, subsystem, platform, force, etc.) is the analysis focused upon?
- What type of measure(s) will answer the decision-maker's question?

1. Example INFOCON Field Experiment Objective

One potential objective of an INFOCON field experiment is to investigate the effect of varying INFOCON levels, under operational conditions, on the war fighter's ability to conduct command and control functions. The goal of the experiment is to highlight how implementation of a defensive network posture will influence command and control decision-making and situational awareness in an operational environment. The effort should include investigations that illustrate inherent vulnerabilities associated with INFOCON's and discussion of experimental objectives aimed at researching the conceptual frame of potential solutions.

2. Example INFOCON Experimental Questions

One hypothesis for a field experiment is that the increasingly restrictive postures associated with progressive INFOCON levels will adversely impact the warfighters' ability to accomplish command and control functions. This implies that the key warfighting capability addressed in the experiment is the ability to accomplish mission tasking in the event of INFOCON implementations. Although specific field experiment capabilities are dependent on the dynamic operational environment, based on pending architectures and scenarios, example experimental questions can still be identified. Several questions are provided for reference.

- What systems do each INFOCON setting impact?
- What impact does INFOCON have on the warfighter's C2 capability?
- What is the increase in time to complete a specific task?

- What work-around does the warfighter employ to complete mission assignments?
- What are the default communication methods during INFOCON implementations?

D. INFOCON SYSTEM BOUNDING AND PROCESS IDENTIFICATION

It is critical that C3 system bounding and C3 process identification within the C3 system of interest are accomplished early in the INFOCON field design. These are MCES Modules 2 and 3, respectively. The INFOCON operational experiment must be structured so that measurement (objective and subjective) of the impact of INFOCON constraints in the field setting can occur. The experiment should provide an opportunity to measure the systems affected by INFOCON's, the impact of INFOCON's on the ability of participants to maintain situational awareness and to conduct effective command and control, and to identify the work-arounds used by warfighters' to complete the mission, if possible, despite INFOCON implementations. C3 system bounding enumerates the relevant system elements that bound the problem of interest. When bounding the C3 system of interest, one must identify the human, hardware and software entities, and structures that are related to the environment external to the C3 system being evaluated. After identifying the C3 system boundaries, the command and control processes (e.g. interactions between personnel, equipment, etc.) and their functions must be identified. The analyst should focus on the inputs and outputs to the processes under normal conditions so as to understand the adaptive processes that may be incorporated under

various INFOCON threat conditions. The term processes in this context defines the interrelationships of tasks that are performed to fulfill the functions.

As an example, the IA C2 INFOCON laboratory discussed in Chapter IV experiment focused on evaluating the impact of INFOCON on the Battle Watch Staff operating inside the Joint Operations Center (JOC) on a Flagship. The JOC is the focal point for decision-makers aboard a Flagship. However, the majority of the C4I functionality and operations for the Flagship are typically carried out in other operational spaces on ship. Hence, understanding the architecture, information flows, and how the system entities relate to the forces it controls and the environmental stimuli to which it responds (e.g. INFOCON implementations) is essential.

1. Understanding the C4I Architecture, Information Flow and Integration Details

During an INFOCON laboratory setting, the test bed C4I architecture is a compromise between credibility, complexity, and cost effectiveness. The results of the experiment must stand up to both technical scrutiny and even more importantly operator scrutiny. However, the test bed infrastructure, like the one designed for the IO C2 INFOCON laboratory experiment, does not permit the installation of a complete ship C4I suite. Thus, planners are only able to replicate a representative cross section of the fielded computers and communication processes that are integrated on a command ship plus the connecting infrastructure. In contrast, an INFOCON field experiment would be populated with the complete suite of operational systems and driven by real world inputs that stimulate the environment. A thorough understanding of the C4I architecture and

integration (MCES Module 4) issues related to the hardware and software entities to be evaluated during an INFOCON field experiment must be documented prior to the specification of measures. Here, the term architecture is used to describe the output of the integration module and should define interfaces and standards of the C3 system being evaluated. The final form of the architecture and information flow should include the process description of the system elements performing the processes that includes the interrelationships between equipment and humans.

2. Relationship Between Human Factors and Organizational Issues

The analysis of C2 should consider all the relevant command levels and functions involved and should investigate issues of integration across command levels and functional domains over time. Consideration should also be given to the robustness and security of information systems and to human computer interface issues. Both human factors and organizational issues must be included in C2 analyses. (A Guide to Best Practice in C2 Assessment, 1999)

Since INFOCON C2 deals extensively with distributed teams of humans under stress and their decision-making behavior, the structuring of the problem and establishment of the research design cannot be completed without explicit consideration of both human factors and organizational issues. Although all elements of an INFOCON C2 system are ultimately related to one another, the linkage between human factors and organizational issues is particularly direct and close. Organizational design or command structure should reflect the interactions among the tasks to be completed, the humans available to perform them, and the equipment or tools that support those humans. Hence, in large measure the effectiveness of an organization's C2, in varying INFOCON levels,

will depend on the capabilities, training, and experience of the people in the C2 system. Since both human factors and organizational issues can impact C2 performance, efficiency, and effectiveness, analysts must consider their impact early in the experiment design process so measures aimed at obtaining a better understanding of human-in-the-loop issues associated with INFOCON implementations can be developed to better understand this human factors and organizational relationship.

E. INFOCON SCENARIO SPECIFICATION AND SELECTION ISSUES

"The experiment scenario is a description of the area, environment, means, objectives and events related to a conflict or a crisis during a specified time frame suited for satisfactory study objectives and the problem analysis directives." (A Guide to Best Practice for C2 Assessment, 1999) This process of creating the scenario is an art that requires subject matter experts to identify, specify, and refine the scenario throughout the experimental design process. The first step is to identify the range of possible scenarios consistent with the problem structure and relevant human factors. The analysts goal is to identify those key or unique factors that must be included in the scenario so as to provide data collection opportunities that could help answer the analytical questions identified during the problem formulation phase. Next, some experienced analysts prefer to begin with an unbounded scenario set that defines the range of interests. Others have found that they can manage complexity better by specifying a particular set of scenarios of interest. In either case, multiple scenarios usually need to be considered to ensure that the problem is fully addressed. Finally, the analyst must review and refine the initial set of scenarios

to ensure that they cover the range of C2 issues and elements of the problem as well as any anticipated changes in the functional command and control process.

The experiment scenario should incorporate specific events that impact both the INFOCON posture and the participant's ability to perform operational tasks. As an example, the IA C2 INFOCON laboratory experiment highlighted in Chapter IV consisted of a series of five nominal watches. Each successive watch was conducted at an increased INFOCON level and permitted participants to step through critical phases of a real world operational scenario, modified for the experiment, in a controlled snapshot fashion. The scenario for the IA C2 INFOCON laboratory experiment provided a framework within which to measure the impact of INFOCON implementations on a representative Battle Watch team. A similar approach for specifying and selecting scenario options for a field experiment should be explored. However, a unique aspect of the laboratory experiment, as opposed to a field experiment that must be considered is that operational networks supporting the experiment participants in the lab would be, in most cases, isolated from the external world. With this control, analysts can actually show the impact on the C2 systems of the various network attacks included in the scenario, a luxury that may not be available in an operational environment. The C2 systems in the laboratory environment would also accurately reflect the current scenario INFOCON level. That is, data would not flow in the experiment if it would not be there at that particular INFOCON level, another level of control that may not be available when conducting an INFOCON experiment in a field environment.

F. INFOCON MEASURES OF MERIT

No single measure or methodology exists that satisfactorily assesses the overall quality of C2. "The crucial causal and analytic chain for C2 analyses is the linking of dimensional parameters to measures of system performance to measures of C2 effectiveness and measures of force effectiveness." (A Guide to Best Practices for C2 Assessment, 1999) Hence, analysts must specify the measures (MCES module 5) necessary to answer the problem of interest as defined in the problem formulation, system bounding process and integration phases. It is critical that the selection of Measures of Merit (MoM), like any other key step in the C2 methodology, be discussed with the decision-makers participating in the experiment. Their acceptance of this formulation is the beginning of their acceptance of the results of the experiment.

A description of each Measure of Merit was extracted from the Guide to Best Practice for C2 Assessment, and is highlighted below along with a diagram presented as Figure 5-2 that illustrates the relationship between each different class of measures. In addition, several categories of INFOCON experiment measures are described below for reference.

- Measures of Force Effectiveness (MoFE), which focuses on how a force performs its mission or the degree to which it meets its objectives.
- Measures of C2 Effectiveness (MoE), which focuses on the impact of C2 systems within the operational context. Examples include the ability to formulate plans that work to achieve objectives, the capacity to create a common operating picture of the battlespace, and reaction time
- Measures of C2 System Performance, which focuses on internal system structures, characteristics, and behavior. Performance measures of a system's behavior may

be reduced to measure based on time, accuracy, capacity or a combination that may be interdependent.

- Dimensional Parameters (DP) are the properties or characteristics inherent in the physical C2 systems. Examples include bandwidth of communications linkages, signal to noise ratios, and luminosity of display screens in command centers.

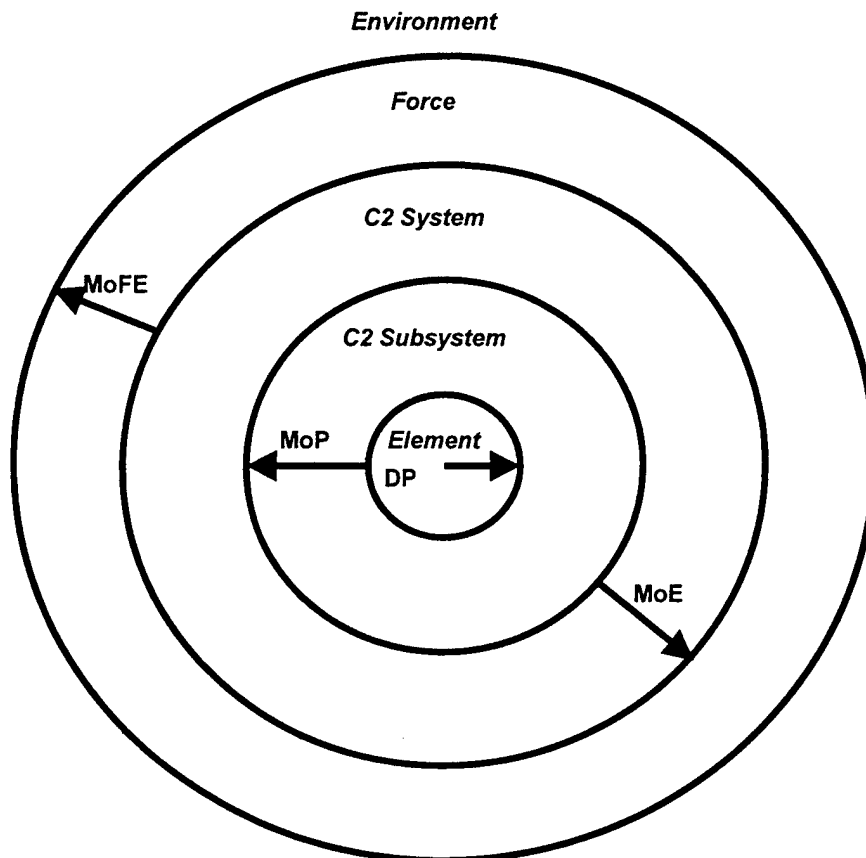


Figure 5-2. Relationship Among Classes of Measures of Merit
(A Guide to Best Practice for C2 Assessment, 1999)

1. Impact of INFOCON on Mission Performance

Analysts should develop a self-report measure that yields insight into the impact in a test subjects ability to perform tasks under varying INFOCON levels. This will provide perspective from each test subject. This assessment should further illustrate the mission activities impacted during an INFOCON implementation and highlight the

potential work-around necessary to complete required tasking under operational conditions. Information about the mission performance level of organizational members could be used to understand and assess intra-cell and inter-cell performance effectiveness across the spectrum of INFOCON levels.

2. INFOCON Workload Assessment with NASA Task Load Index

If possible, subjective estimates of workload should be elicited from each participant using experiment specific NASA Task Load Index (TLX) questionnaires. NASA TLX is a subjective workload assessment tool that allows users to perform subjective workload self-assessment while working with various human-machine C3 systems. As described earlier, TLX is a multi-dimensional rating procedure that derives an overall workload score based on weighted average of ratings on six sub-scales. These sub-scales include Mental Demands, Physical Demands, Temporal Demands, Own Performance, Effort, and Frustration. NASA TLX is a good tool to use during INFOCON experimentation efforts because it can be used to assess workload in various human-machine C3 environments and other process control environments.

Appendix D, TLX Assessment Instruments, provides examples of the instruments used during the IO C2 INFOCON laboratory experiment that was discussed in Chapter IV. The questionnaire in Appendix D elicits participant estimates of their own workload and of the workload experienced by other cells. In addition to yielding information about the perceived workload of individuals and cells in the organization, the measure can also be used to derive information about the balance or variability of workload across the

organization during an INFOCON implementation. This information is valuable because it can be used to distribute workload differently during each particular INFOCON. It can also be used to increase the participant's knowledge of dynamic organizational procedures and processes.

3. Relationship between INFOCON and Situational Awareness

In general, situational awareness (SA) refers to the decision-makers moment-by-moment ability to monitor and understand the state of the complex system and its environment. Developing SA includes understanding many factors, including the commander's intent, mission, enemy intent, C4I architecture, information flow, etc. Generally speaking, the concept of SA refers to the mental process of knowing what is going on at any point and time in the surrounding environment. "SA is important in military decision-making for several reasons. It provides the foundation for subsequent decision-making and action selection in complex, dynamic environments." (Kemple and Hutchins, 1999) When emergencies arise, the completeness and accuracy of the decision-makers SA are critical to the ability to make decisions, revise plans, and manage the system.

During an INFOCON, many factors can degrade an individual's SA, such as, information ambiguity, cognitive overload and human error, loss of communications or other information sources, and time delay in information receipt. Instruments should be developed to capture the effect of each factor on a participant's ability to complete mission tasking. For many C2 experiments, including INFOCON, there may be no

existing measurement instrument available to clearly answer the question of interest. However, a methodology should be designed that will provide a measure of each participants ability to ascertain what occurred during a particular period of time in all specific areas of concern. It should be noted that developing a useful measurement instrument requires both creativity and an understanding of measurement theory. However, having an abundant supply of both these qualities does not necessarily guarantee success in truly understanding participants' situational awareness during a particular event.

4. Instrumentation

Instruments useful for performance measurement require a balance between experimental control on the one hand and operational realism on the other. "Experimental control refers to the ability to structure the environment so that the data obtained will be clearly interpretable. It means the environment presented to the participants needs to be controlled so that extraneous factors (intervening variables) do not cloud the picture by influencing performance in ways that are not intended while, at the same time, ensuring that the scenario is not so sterile that operational realism is missing." (Kemple and Hutchins, 2000) Experimental control includes the idea that the measurements need to be valid within the experimental setting while reliably capturing data that will provide answers to the question's of interest. Reliability refers to the idea that if the same events occur, the values should be relatively similar. Validity refers to the degree to which the measurement instrument actually measures what it was designed to measure. Validity

tests how well the measurement instrument fulfills its function. Operational realism requires that the measurement instruments not intrude upon the decision-makers process.

G. DATA COLLECTION AND ANALYSIS STRATEGY

Capturing experiment data and results is complex in concept, planning, and execution. However, if the experiment measures are correctly specified and correlated with the experimental question, then capturing the required data (MCES module 6) should result in answers to those questions. In planning, analysts have to become familiar with the dynamic conceptual terrain of the experiment. "As an added challenge, it is necessary that as concepts are developed and coupled to experimentation, that there exists some correspondence between the intent of the experiment, the concept being considered in planning the experiment, and data collected in the conduct of the experiment." (Schacher and Gallup, 2000) In general, this has meant that concepts have had to be re-defined as a set of questions, and that these derived questions must be related to those elements of data that would suffice to expand knowledge about the question and therefore the concept being considered. For this reason, it is important that data collectors understand the conceptual terrain of their respective observation areas and the related questions.

Besides this concept-question-data instrument process, there are other very important data requirements. First, the questions defined during the problem formulation phase must be refined through the experiment. That is, based on the conduct and results of the experiment, a feedback mechanism should be implemented that identifies questions

that surface as a result during the experiment. These should be captured for further exploration. Second, innovation must not be neglected as a source of data. The data and analysis plan is the detailed plan that includes what data will be captured, by what capture means, at which experiment nodes, and what information will be produced from analysis.

That said:

The data capture plan is a proposal about what might be important, based on what has been defined as relevant questions, and may be observed in what is thought to be the probable set of activities in the experiment. It is certainly possible that there will be a completely different set of activities, or 'unexpected results', and these are often the most relevant and important results of an experiment. Data collectors must be sensitive to these occurrences, noting them with as much explanation as possible. (Schacher and Gallup, 2000)

The INFOCON experiment observers should obtain qualitative and quantitative measures of activities as the test subjects engage various scenarios in a field setting. The observers working with the participants should do the primary data collection during an INFOCON field experiment. The observers should take notes to document observations concerning task performance in various levels of INFOCON, and the participants should have computer aided questionnaires to complete during the experiment that are aimed at quantifying subjective comments. Data should provide analysts with diagnostic information that may lead to a better understanding of the impact of setting INFOCON on situational awareness and the command and control process. To carry out this effort, the analysts should develop a small set of diagnostic measures that are based on reliable instruments and procedures that have been used successfully in previous INFOCON laboratory experiments. In addition, the C4I infrastructure should be instrumented (e.g.

server load monitoring, keystroke capture capability, etc.) to augment the observations with value added objective data. Understanding the intended data flow in the C4I architecture and the primary paths used to share information products should dictate where network instrumentation should be integrated. This equipment should be implemented to provide the statistical data set required when assessing information flow within the system under normal conditions as well as during various INFOCON implementations.

Data aggregation is the final module (Module 7) in the MCES framework. For this effort, it addresses the issue of how the analyst will interpret the measures incorporated to better understand the implications of implementing INFOCON's on a command and control structure.

The implementation of this module provides the analytical results tailored to address the problem posed at the beginning of the procedure. The results, made up of the aggregated values and measures should be provided to the decision maker in a format that will expedite his consideration of the analyses. (Sweet, 1986)

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY

Information Operation Condition (INFOCON) implementations and specifically the impact these implementations can have on warfighting command and control processes are not yet widely understood or appreciated by the majority of the operating forces. INFOCON actions are designed to heighten or reduce defensive posture uniformly, to defend against computer network attacks, and to mitigate sustained damage to the DoD infrastructure. Experimentation is required to explore the effects on certain command and control processes under various INFOCON conditions. This thesis explored requirements for conducting these INFOCON experiments and resulted in the development of an INFOCON experimental design methodology that can be used as a framework for designing and conducting INFOCON experiments in the field. INFOCON experimentation efforts will provide insight and a better understanding of the effects that these implementations have on the ability of a commander to conduct seamless command and control functions after such conditions are instituted.

The primary hypothesis associated with INFOCON implementation and articulated in this thesis is that the increasingly restrictive posture associated with progressive INFOCON levels will adversely impact the warfighters' ability to accomplish command and control tasks in a network centric environment. Although the data set collected during the IO C2 INFOCON laboratory experiment, discussed in Chapter IV, was relatively small, the results supported this hypothesis. However, experimentation aimed at researching INFOCON effects on command and control processes in an

operational setting is still required to better understand the real world effects of imposing such conditions. Hence, as mentioned above, this thesis focused on developing the framework to conduct an operational INFOCON experiment. That framework is discussed in Chapter V. The two primary research questions addressed in this thesis were:

- How can the effects of INFOCON be evaluated in an operational environment?
- What is an INFOCON experimental design framework for measuring the impact of INFOCON implementations on command and control in an operational setting?

In order to thoroughly answer the research questions, this thesis was divided into six chapters including the Introduction and this Summary. Chapter II provided an overview of the Network Centric Warfare concept and discussed the requirements and challenges of maintaining information dominance in a Network Centric Warfare environment. It also gave the reader a broad overview of issues related to computer network vulnerabilities and discussed the challenges associated with protecting military networks from adversarial attack and highlighted actions that could be taken in such an event.

Chapter III introduced the Information Operation Condition system and provided the reader with a complete description of the INFOCON defensive Information Operations (IO) action. As discussed in chapter III, the INFOCON is a comprehensive defensive posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. In addition, this chapter highlighted the keys to successful INFOCON implementation. It emphasized

the importance of reviewing and testing INFOCON actions often to help personnel understand their roles and responsibilities, determining the effects of responsive measures as they relate to command and control decision making, and detecting problems in existing INFOCON procedures.

As an initial step to better understanding the impact INFOCON implementations have on command and control functions in an operational setting, a controlled laboratory experiment, in which the author participated, was conducted at the SPAWAR Information Operations Center of the Future. The analysis of this initial INFOCON laboratory experiment was detailed in Chapter IV. The primary objective of this experiment was to investigate the relationship between military INFOCON implementations and their impact on the warfighter's ability to conduct operational command and control tasks. This laboratory experiment identified important information relating to situational awareness and command and control effectiveness that should be considered prior to imposing INFOCON in a real world field environment.

Research and experiment planning for this effort provided information regarding how the effects of INFOCON can be evaluated in an operational environment, the first thesis question. Results from this experiment indicate that as the INFOCON level is increased, workload impact and time to complete functional tasks also increases, while battle space situational awareness decreases. Data collected during this laboratory experiment and discussed in Chapter IV indicate that the effects of INFOCON can be evaluated by measuring a participant's workload impact, situational awareness, and time delta to accomplish specific tasks under varying INFOCON situations. Instruments

developed for this laboratory experiment are presented in Appendix D and could be used as a guide to measure the same command and control effects during a field experiment.

Chapter V provides the INFOCON experimental framework for measuring the impact of INFOCON implementations on command and control functions in an operational environment, the second thesis question. The author chose to use the Modular Command and Control Evaluation System (MCES) as the basis for discussing an INFOCON experiment in a field setting because it provides a process to evaluate C3 systems and architectures. The framework developed to conduct an INFOCON experiment in a field setting was centered on the MCES process. This process will help planners and analysts develop an experimental design that will ultimately capture the data required to support the analysis of the relevant experimental questions. The MCES presents a method to attack difficult concepts like INFOCON in a standardized manner and was used as a guide to develop the INFOCON experimental design methodology discussed in this section.

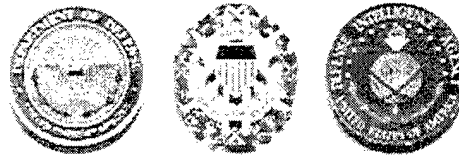
In summary, the critical role of global networks to support military operations makes the development of effective infrastructure protection the utmost importance to naval forces. The INFOCON system provides DoD elements with a structured, standardized approach to defend against and react to attacks on computer systems and networks. Although much was learned about the effects of imposing INFOCON on an organizations command and control process from the initial INFOCON laboratory experiment, the test environment was artificial. Therefore, subsequent experimentation in an operational environment is needed to better understand the impacts that setting

INFOCON's will have on real world tasking. The methodology developed for this thesis should be used during planning efforts for just such an operational experiment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. JCS INFOCON MEMORANDUM

*Information Operation
Condition*



CM-510-99
10 March 99

UNCLASSIFIED

Subject: Information Operations Condition

1. (U) This memorandum establishes the Information Operations Condition (INFOCON) for the Department of Defense. The system presents a structured, coordinated approach to react to and defend against adversarial attacks on DoD computers and telecommunications. Specific guidance and responsibilities for authorizing and communicating INFOCON's as part of information operations throughout the Department of Defense are provided at the enclosure.
2. (U) INFOCON applies to the Joint Staff, Services, combatant commands, and Defense Agencies -- as well as joint, combined, and other DoD activities throughout the entire conflict spectrum -- peacetime through war. These procedures are effective immediately and will remain in effect until superseded by DOD instruction. Addressees have 60 days from the date of this memorandum to develop procedures in compliance with the Enclosure, if required.
3. (U) Joint Staff point of contact is Major Felipe Morales, J-3, (703) 693-4698 or DSN 223-4698.

Signed

JOSEPH W. RALSTON

Acting Chairman
of the Joint Chiefs of Staff

UNCLASSIFIED

THIS PAGE INTIONALLY LEFT BLANK

APPENDIX B. INFOCON STRUCTURE

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
<p>NORMAL</p> <p>NORMAL ACTIVITY</p>	<p>No significant activity.</p>	<ul style="list-style-type: none"> - Ensure all mission critical information and information systems (including applications and databases) and their operational importance are identified. - Ensure all points of access and their operational necessity are identified. - On a continuing basis, conduct normal security practices. For example: <ul style="list-style-type: none"> - Conduct education and training for users, administrators, and management. - Ensure an effective password management program is in place. - Conduct periodic internal security reviews and external vulnerability assessments. - Conduct normal auditing, review, and file back-up procedures. - Confirm the existence of newly identified vulnerabilities and install patches. - Employ normal reporting procedures IAW para 7d. - Periodically review and test higher level INFOCON actions.
<p>ALPHA</p> <p>INCREASED RISK OF ATTACK</p>	<ul style="list-style-type: none"> - Indications and warning (I&W) indicate general threat. - Regional events occurring which affect US interests and involve potential adversaries with suspected or known CNA capability. - Military operation, contingency or exercise planned or ongoing requiring increased security of information systems. - Information system probes, scans or other activities detected indicating a pattern of surveillance. 	<ul style="list-style-type: none"> - Accomplish all actions required at INFOCON normal. - Execute appropriate security practices (see Appendix A). For example: <ul style="list-style-type: none"> - Increase level of auditing, review, and critical file back-up procedures. - Conduct internal security review on all critical systems. - Heighten awareness of all information system users and administrators. - Execute appropriate defensive tactics (see Appendix B) - Employ normal reporting procedures IAW para 7d. - Review and test higher level INFOCON actions, and consider proactive execution.
<p>BRAVO</p> <p>SPECIFIC RISK OF ATTACK</p>	<ul style="list-style-type: none"> - I&W indicate targeting of specific system, location, unit or operation. - Major military operation or contingency, planned or ongoing. - Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance. - Network penetration or denial of service attempted with no impact to DOD operations. 	<ul style="list-style-type: none"> - Accomplish all actions required at INFOCON ALPHA. - Execute appropriate security practices (see Appendix A). For example: <ul style="list-style-type: none"> - Increase level of auditing, review, and critical file back-up procedures. - Conduct immediate internal security review on all critical systems. - Confirm existence of newly identified vulnerabilities and install patches. - Disconnect unclassified dial-up connections not required for current operation. - Execute appropriate defensive tactics (see Appendix B) - Ensure increased reporting requirements are met IAW para 7d. - Review and test higher level INFOCON actions, and consider proactive execution.

APPENDIX B. INFOCON STRUCTURE

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
<p>CHARLIE LIMITED ATTACK(S)</p>	<ul style="list-style-type: none"> - Intelligence attack assessment(s) indicate a limited attack. - Information system attack(s) detected with limited impact to DOD operations: - Minimal success, successfully counteracted. - Little or no data or systems compromised. - Unit able to accomplish mission. 	<ul style="list-style-type: none"> - Accomplish all actions required at INFOCON BRAVO. - Execute appropriate response actions. For example: - Conduct maximum level of auditing, review and critical file back-up procedures. - Consider minimize on appropriate computer networks and telecommunications systems (limit traffic to mission essential communication only). (See Appendix E, ref. e, CJCSI 6900.01A) - Reconfigure information systems to minimize access points and increase security. - Reroute mission-critical communications through unaffected systems. - Disconnect non-mission-critical networks - Employ alternative modes of communication and disseminate new contact information. - Execute appropriate defensive tactics (see Appendix B). - Ensure increased reporting requirements are met IAW para 7d. - Review and test higher level INFOCON actions, and consider proactive execution.
<p>DELTA GENERAL ATTACK(S)</p>	<ul style="list-style-type: none"> - Successful information system attack(s) detected which impact DOD operations. - Widespread incidents that undermine ability to function effectively. - Significant risk of mission failure. 	<ul style="list-style-type: none"> - Accomplish all actions required at INFOCON CHARLIE. - Ensure increased reporting requirements are met IAW para 7d. - Execute applicable portions of continuity of operations plan (See Appendix E, ref. f, DODD 3020.26, Continuity of Operations, Policy and Planning). For example: - Designate alternate information systems and disseminate new communication procedures internally and externally. - Execute procedures for ensuring graceful degradation of information systems. - Implement procedures for conducting operations in "stand-alone" mode or manually. - Isolate compromised systems from rest of network. - Execute appropriate defensive tactics (see Appendix B).

APPENDIX C. COMTHIRDFLT INFOCON STANDARD OPERATING PROCEDURES

Date Originated: 01 Nov 99

Title: COMTHIRDFLT/USS CORONADO (AGF-11) INFOCON STANDARD OPERATING PROCEDURE

Subject: INFOCON IMPLEMENTATION AND REPORTING PROCEDURES

Reference: a. CINCPACFLT 220536Z AUG 98 (INFOCON SOP)

b. CINCPACFLT 312056Z AUG 98 (Incident Reporting procedures)

Purpose: This policy details the Commander Third Fleet's implementation and reporting procedures of Information Condition (INFOCON) levels. These INFOCON's typify threat Information Operations (IO) activity at each INFOCON level and corresponding response measures to increase the defensive IO readiness of the entire AOR or a specific sub-region, depending on the IO threat. This SOP provides guidance to all ships under Commander Third Fleet.

Discussion: The decision to increase the INFOCON level is not a stand-alone process. Commander Third Fleet will establish INFOCON's within the AOR based on Network Incident Reports, Fleet Information Warfare Intrusion Incident Reports (IIR), Navy Computer Network Defense (CND) Network Incident Advisory messages, and JTF CND Network Incident Advisory or when directed by higher authorities. INFOCON's are NORMAL, ALPHA (Low Activity), BRAVO (Significant Activity), CHARLIE (Serious Activity), and DELTA (Critical Activity). These levels are analogous to THREATCON levels. Events that would raise or lower those levels may directly affect the existing INFOCON level. However, INFOCON's are independent from DEFCON and THREATCON levels. Commander Third Fleet could declare a higher INFOCON level without the declaration of a higher DEFCON or THREATCON level.

INFOCON: Commander Third Fleet is the INFOCON declaration authority for all ships assigned under C3F. Establishing an INFOCON does NOT presuppose all response measures within the declared INFOCON will be activated. Upon declaration of INFOCON ALPHA or higher, C3F will direct specific defensive measures for implementation within the theater (e.g. Alpha measures 1-13, Bravo 1-35, Charlie measures 1-44, and Delta measures 1-47). Directed action may include measures from a higher INFOCON. For example, while in INFOCON ALPHA, C3F may direct additional measures listed for INFOCON BRAVO.

a. INFOCON's and response measures apply to all GENSER and SCI Information Systems (i.e. NIPRNET, SIPRNET, Coalition Wide-Area Network (CWAN) and JWICS) within C3F AOR.

b. The threat IO activity described in each INFOCON, and the corresponding responses are not all inclusive. Each unit commander should review these measures for applicability and determine if additional response measures are required as well as promulgating amplifying instructions if necessary. Additionally, as technology changes, these measures should be reviewed periodically to account for vulnerability changes.

INFOCON LEVELS:

a. INFOCON NORMAL - This day to day condition warrants established routine security procedures. Typical threat IO activity at this level includes random surveillance or reconnaissance probes on Commander Third Fleet's information infrastructure. Foreign press and public diplomacy activities are routine. At this level, daily information system security measures apply including automated 24 hour/day monitoring of critical command, control, and communication systems. FIWC provides 24 hour/day monitoring of CINCPACFLT and PRNOC Information Systems on NIPRNET and SIPRNET.

b. INFOCON ALPHA (Low Activity) - This condition is declared when a general threat of information attack against Commander Third Fleet exists. Typical threat IO activity at this level includes computer network scans, probes, or mapping, which might indicate an increased surveillance or reconnaissance against C3F's information infrastructure. Limited computer network attacks, with no operational impact, could also be expected at this INFOCON

APPENDIX C. COMTHIRDFLT INFOCON STANDARD OPERATING PROCEDURES

level. Other forms of threat IO activity could include public diplomacy efforts by an adversary to undermine U.S. regional interests and policy. Action addressees should be able to maintain response activity at this INFOCON for an indefinite period of time.

c. INFOCON BRAVO (Significant Activity) - This condition is declared when a specific threat of an information attack against Commander Third Fleet exists. This condition may be prompted by information warfare (IW) threat warning assessment indicating specific adversary capabilities with evidence of intent. Typical threat IO activity at this level includes limited computer network attacks with operational impact. Additional indicators include: increased anti-U.S./western rhetoric, leaflet campaigns, public demonstrations, public speakers, "Internet rumors," or media reports counter to U.S., U.S. allies, or U.S. coalition partners. Other indicators may include a significant increase in detected viruses, or limited denial of service attacks. Action addressees should be able to maintain response activity at this INFOCON for several weeks without undue personnel hardships or degrading Commander Third Fleet's ability to operate.

d. INFOCON CHARLIE (Serious Activity) - This condition applies when an actual information attack occurs with significant operational impact. This condition could also apply when intelligence indicates the possibility of an imminent information attack against a Commander Third Fleet target with potential operational impact. Typical threat IO activity at this level includes actual or threatened attempts to gain access to Commander Third Fleet computer network systems for the purpose of massive data destruction, false data creation, wide denial of service, or gaining control of critical systems. The injection across several networks of malicious code (i.e., viruses, worms, Trojan horses, etc.) and e-mail bombs all fall into this INFOCON. At this INFOCON level, entities acting either singularly, aligned, or in unprecedented coalitions, can be expected to counter U.S. policy through intense and broad regional press and public diplomacy. Response measures at this INFOCON are focused at protecting Commander Third Fleet's forces' ability to operate as needed. When implemented for even short periods of time, response measures at this INFOCON could create personnel hardship, affect peacetime activities, and have the potential for increased operational costs.

e. INFOCON DELTA (Critical Activity) - This condition applies when DEFCON and/or THREATCON levels exist to warrant extreme measures, or when the severity of an information attack against Commander Third Fleet significantly degrades readiness and operations. Extensive coordinated regional and global information attacks or slanders by entities with hostile intent toward/against the U.S. and its allies are expected, to include exposé in the media, international forums, and over the Internet which are counter to U.S. policy and interests. Response measures at this INFOCON are focused on maintaining or restoring systems critical to Commander Third Fleet's ability to operate. As with INFOCON CHARLIE, action addressees will likely experience personnel hardships, increased operational costs (both time and dollars) and degradation in their peacetime activities.

Action:

ALPHA 1-13

1. Call a meeting of the C3F Information Assurance (IA) Cell Working Group to inform them of the IO activity and immediate actions being taken. (*IA Cell*)
2. Update points of contact list of phone numbers, e-mail addresses, and official message address list. (*All Hands*)
3. Alert J6, Information System Security Managers (ISSMs) and Departmental Information System Security Officers (ISSOs) of increased threat condition. (*ISSM*)
4. Issue threat assessments of suspected IO activities and identify suspected friendly targets vulnerable to IO attacks. (*ISSM, J6*)
5. Ensure all ISSMs, ISSOs, and System Administrators (SA) are briefed on the threat IO activity and response measures. (*ISSM*)
6. Increase OPSEC awareness. (*IW Protect Officer*)

APPENDIX C. COMTHIRDFLT INFOCON STANDARD OPERATING PROCEDURES

7. Remind all users to be particularly suspicious of anyone requesting passwords for direct access to C4ISR systems. (*All Hands*)
8. Remind all users that scanning computer disks for viruses is mandatory prior to use in PACFLT AOR computers. (*All Hands*)
9. Remind all users to report unusual activity, viruses, and potential denials of service of computer or telephone systems including FAXs. Report unusual activity in accordance with established **C3F Computer Network Incident reporting procedures**. (See also CINCPACFLT message DTG 312056ZAUG98) (*ISSM, ISSO, NSO*)
10. Validate the operation of server system log files, and in addition to daily reviews, review network monitoring logs, system audit logs, and server system log files for evidence of specific malicious activity. Specifics will be provided in the INFOCON implementation message, and based on the actual situation. (*NSO*)
11. Contact CPF to ensure routers and firewalls protecting all segmented critical C4ISR systems have proper configuration settings to guard against known vulnerabilities and methods of recent attacks. (*NSO*)
12. Remind all users that external unclassified E-mail access such as Hot Mail, Yahoo Mail, or "popping for mail" is prohibited on COMNAVSURFPAC computers.
13. Remind all users that Internet Chat Rooms, Messengers, Stock or News Tickers are prohibited on C3F/USS CORONADO computers. (*All Hands*)
- BRAVO 1-35**
14. Ensure all telephone instruments are at least 3 feet from computers handling classified material. (*ISSOs*)
15. Update and disseminate list of essential elements of friendly information (EEFI). (*IW Protect Officer*)
16. ISSMs, ISSOs and SAs will remind users of the need for passwords with a minimum of 8 random alphanumeric characters. This is to counter attempts to crack passwords with very large dictionary files. (*ISSM, ISSO, NSO*)
17. Conduct periodic internal security reviews and external vulnerability assessments of C4ISR systems. (C3F *ISSM, ISSO, NSO, SA*) **Reassess 8, 10 and C3F's minimum computer security requirements are implemented**
18. Verify latest software patches/versions have been installed; coordinate with CPF, PRNOC, NAVCIRT and INFOSEC homepages. (*ISSM, NSO/CPF N69*)
19. Identify critical computer files and review back-up procedures for those files. (*NSO, SA*)
20. Confirm updated computer virus signatures are loaded and run virus detection/eradication software. (*NSO, SA*)
21. At least once every 30 days, Network Security Officer will run available password cracker program, or an equivalent program, to detect and correct weak passwords. (*NSO, SA*)
22. Direct all ISSMs, ISSOs, and SAs to increase their security awareness, particularly for critical C4ISR systems and place them on alert for possible recall after normal duty hours. (*ISSM, ISSO, SA*)
23. Verify real-time audit capabilities, if available, are turned on. (*NSO, SCI SA*) *N/A*
24. Verified CPF has closed all remote maintenance ports on routers, firewalls, servers, and electronic phone switches. (*ISSM*)
25. Review options and operational impacts of disconnecting all bridges between unclassified and classified networks, such as Secure Mail Guard (SMG) (this is the software portion) between unclassified and classified LANs. (*IA Cell*)
26. IA Cell determines who are the NIPRNET operational users (i.e., CMOC, disbursing, medical and supply). Depending on the threat indicators, allow only operational users on NIPRNET, disconnect NIPRNET from the World Wide Web or secure NIPRNET completely. (*IA Cell*)
27. Verify there are no unclassified dial-out capabilities from LAN workstations. (*ISSO, SA*)

APPENDIX C. COMTHIRDFLT INFOCON STANDARD OPERATING PROCEDURES

- 28. Isolate compromised systems/local network from rest of wide area network. (*ISSM, ISSO, NSO*)
- 29. As appropriate, implement alternate FAX numbers in response to denial of service attacks on FAXs. (*Communications Officer*)
- 30. Conduct computer network vulnerability assessments to re-verify levels of information security. (*ISSM, ISSO, NSO/CPF N69 Need checklist*)
- 31. Verify port security posts guards on secondary power generation equipment for critical command and control centers within C3F AOR. (*Physical Security Manager*)
- 32. When appropriate, direct all NSO and SAs to zero logins and force all accounts to enter new passwords. ISSMs, ISSOs, and SAs will remind users of the need of passwords with a minimum of 8 random alphanumeric characters. (*ISSM, ISSO, SA, NSO*)
- 33. Verify compromised or unauthorized computer system accounts are frozen or eliminated. (*NSO*)
- 34. Remove dial-in access to classified LANs not required for current operations. (C3F) *N/A*
- 35. In the event of an actual computer network attack, users of the affected terminals, and the respective ISSM and ISSO, will isolate the affected terminal or network, ensure evidence is maintained to pass to law enforcement agencies, and then attempt to clean and recover the terminal/network. (*ISSM, ISSO, NSO, SA*)

CHARLIE 1-44

- 36. For the conduct of official business, use only classified mediums of information exchange where feasible, such as secure telephones (STU-IIIs), secure FAXs, and SIPRNET based systems such as Global Command and Control System (GCCS). (*All Hands*)
- 37. Disconnect Secure Mail Guards (SMG) between unclassified and classified LANs. (*J6*)
- 38. Review current IDS coverage and expand to additional computer networks, if operationally feasible. (*NSO*) *N/A*
- 39. Physically disconnect the Secure Gateway Systems to isolate classified LANs. (*J6*)
- 40. Review options, and impacts of, disconnecting all critical C4ISR systems capable of operating in a stand-alone mode. (*IA Cell*)
- 41. Increase monitoring and audit review of Flag officer accounts. For those flag officer systems not in use, secure the hard drives. (*NSO*)
- 42. Conduct maximum level of auditing. (*NSO*)
- 43. Reroute mission critical communications through unaffected systems. (*J6*) *N/A*
- 44. Disconnect non-mission critical C4ISR systems. (*J6*)

DELTA 1-47

- 45. Disconnect all critical C4ISR systems from the network that are capable of operating in a stand-alone mode. (*J6*)
- 46. Remove all hard drives from systems not in use. (*J6*)
- 47. Execute continuity of operations plans, and disseminate new contact information. (*IA Cell*)

REPORTING:

- a. Commander Third Fleet will inform CINCPACFLT N69, FIWC (NAVCIRT) and NCTAMS PAC upon Commander Third Fleet's declaration of an INFOCON level. Primary reporting means will be via official message traffic.
- b. Subordinate commands will notify C3F within four hours of any change in INFOCON level.
- c. Classification. Definition of INFOCON levels, and response measures when linked to a specific INFOCON level or specific IO threat, are classified Secret.

Submitted by: _____ Reviewed by: _____
Approved by: _____

APPENDIX D. WORKLOAD INSTRUMENTS

TLX Factoring: Part A

First, before we start the experiment, think about the work you typically perform at your computer workstation during normal operational conditions at sea. Then, using the TLX Work Scale Definitions that you just read, think about which of the following aspects of your work are the **most important** contributors to **your workload** during a typical operational day.

MENTAL DEMAND	= MD
PHYSICAL DEMAND	= PD
TEMPORAL DEMAND	= TD
EFFORT	= EF
PERFORMANCE	= OP
FRUSTRATION LEVEL	= FR

With that in mind, and using the two letter codes above, choose the one letter pair from each pairing below that is most important to your workload (workload centrality). In other words, if the physical demand (PD) of your typical workload is more important each day than the mental demand (MD), circle the PD in the upper left pairing below. Continue to make your choices for all 15 pairings.

PD / MD	TD / PD	TD / FR
TD / MD	OP / PD	TD / EF
OP / MD	FR / PD	OP / FR
FR / MD	EF / PD	OP / EF
EF / MD	TD / OP	EF / FR

Date/Time: _____

Workstation: _____

APPENDIX D. WORKLOAD INSTRUMENTS

TLX Factoring: Part B

Next, think about the work you typically perform at your computer workstation during normal operational conditions at sea. Then, using the TLI Work Scale Definitions that you read previously, think about which of the following aspects of your workload **change the most** during a typical operational day.

MENTAL DEMAND	= MD
PHYSICAL DEMAND	= PD
TEMPORAL DEMAND	= TD
EFFORT	= EF
PERFORMANCE	= OP
FRUSTRATION LEVEL	= FR

With that in mind, and using the two letter codes above, choose the one letter pair from each pairing below that changes the most (workload variation). In other words, if the physical demand (PD) of your typical work varies more each day than the mental demand (MD), circle the PD in the upper left pairing below. Continue to make your choices for all 15 pairings.

PD / MD	TD / PD	TD / FR
TD / MD	OP / PD	TD / EF
OP / MD	FR / PD	OP / FR
FR / MD	EF / PD	OP / EF
EF / MD	TD / OP	EF / FR

Date/Time: _____

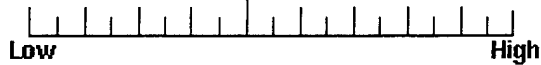
Workstation: _____

APPENDIX D. WORKLOAD INSTRUMENTS

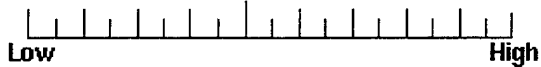
Task Load Index Rating Scales

Use the following six scales to evaluate [1=(LOW) to 10 =(HIGH)] the work you have been doing during the past few hours. Place a check mark (✓) on each line below, and also write the corresponding whole number (1 through 10) to the right of each scale.

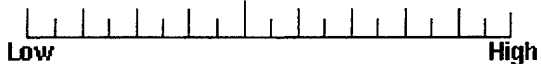
MENTAL DEMAND



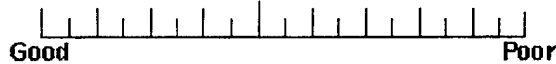
PHYSICAL DEMAND



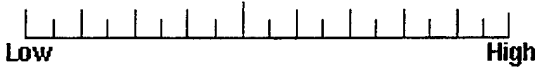
TEMPORAL DEMAND



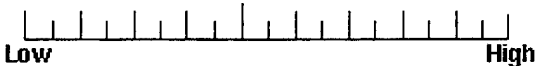
PERFORMANCE



EFFORT



FRUSTRATION



Low / Poor = 1

High / Good = 10

At this time, what is your most important task: _____

Using a scale from 1 (poor) to 10 (excellent), what is your current task-related Situation Awareness level: _____

At this time, what is your estimate of the amount of **INCREASED** time that it will take you to complete your task for this scenario (range from zero to hrs. or days):

Date: _____ Time: _____

INFOCON Level: _____ Workstation: _____

APPENDIX D. WORKLOAD INSTRUMENTS

POST EXPERIMENT CONSIDERATIONS: I

PLEASE PRINT

The findings from this and two other experiments will be written up and put into a report that will be circulated to the project sponsors. Note: no names of individuals who participated in the experiments will be mentioned. However, it is appropriate to include some information that describes the people who provided the data. That is because any report will have different implications if the findings are based on college sophomores, as opposed to military officers, etc.

The information obtained in the three IA C2 experiments this Year will be grouped or combined and reported as averages. We will comply with the Privacy Act (5 U.S.C. 301), and no one's personal information will be disclosed.

What is your (please print):

Military Rank: _____
Years of Military Service: _____
Age: _____
Gender: _____
Military Designator/MOS/Rating (primary) Number: _____
Military Designator/MOS/Rating (secondary) Number: _____
Military Designator/MOS/Rating (tertiary) Number: _____

Describe the formal IA training you have received, and when:

What has been your best source of IA learning or training:

What types of IA training do you, and others in your Designator/MOS/Rating require?
Be specific: _____

Continue to the next page.

APPENDIX D. WORKLOAD INSTRUMENTS

POST EXPERIMENT CONSIDERATIONS: II

PLEASE PRINT

Given your typical at sea work position and operational tasking, in your opinion:

1. At what level of INFOCON (Alpha, Bravo, Charlie, Delta) would you (or other military personnel who work in your position) first notice an impact on your ability to complete your work in a timely manner.

2. At what level of INFOCON (Alpha, Bravo, Charlie, Delta) would you (or other military personnel who work in your position) notice a significant impact on your ability to complete your work in a timely manner.

3. At what level of INFOCON (Alpha, Bravo, Charlie, Delta) would you (or other military personnel who work in your position) be unable to complete your work in a timely manner

4. What computer software tools do you use most often to accomplish your work:

5. What computer networked systems do you use most often to accomplish your work:

6. What is the source for most of the information you need to accomplish typical mission related tasks at sea:

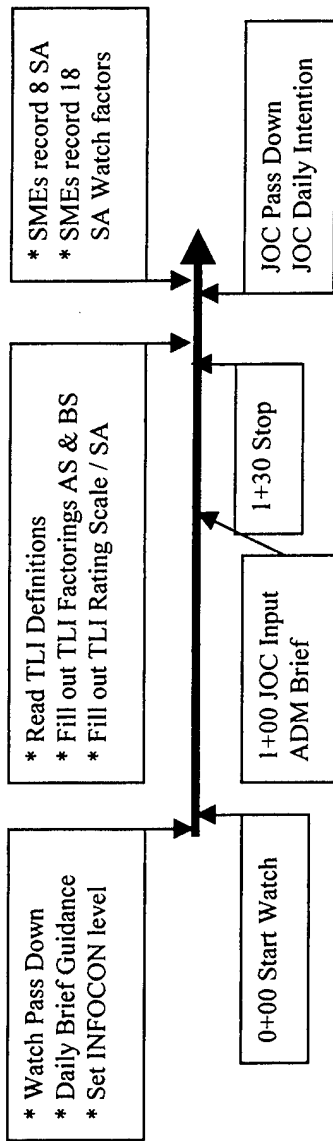
7. Where do you send most of the information you process during a typical mission at sea: _____

8. What other types of work at your command will most likely be impacted by INFOCON's, and then try to estimate the seriousness of those impacts:

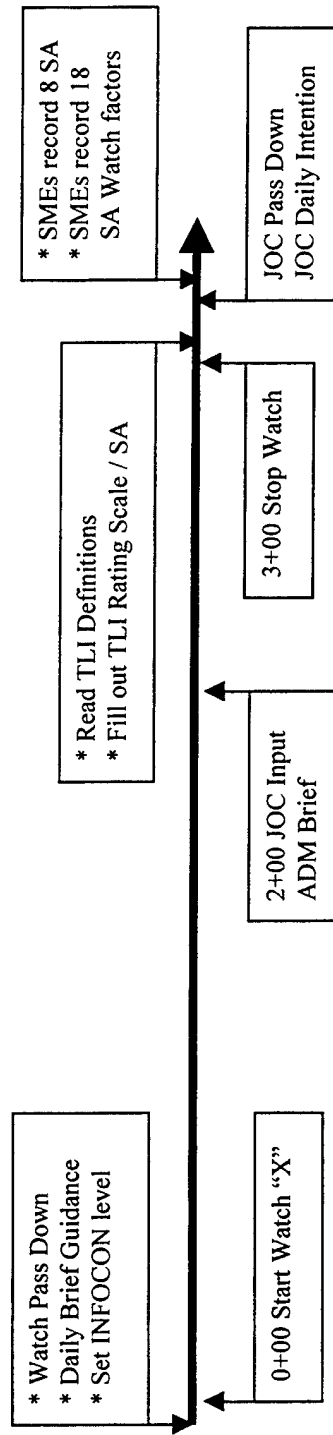
9. Include any comment below that you believe will be useful to the topics of INFOCON's or these IA experiments (continue on the back side if necessary).

THIS PAGE INTENTIONALLY LEFT BLANK

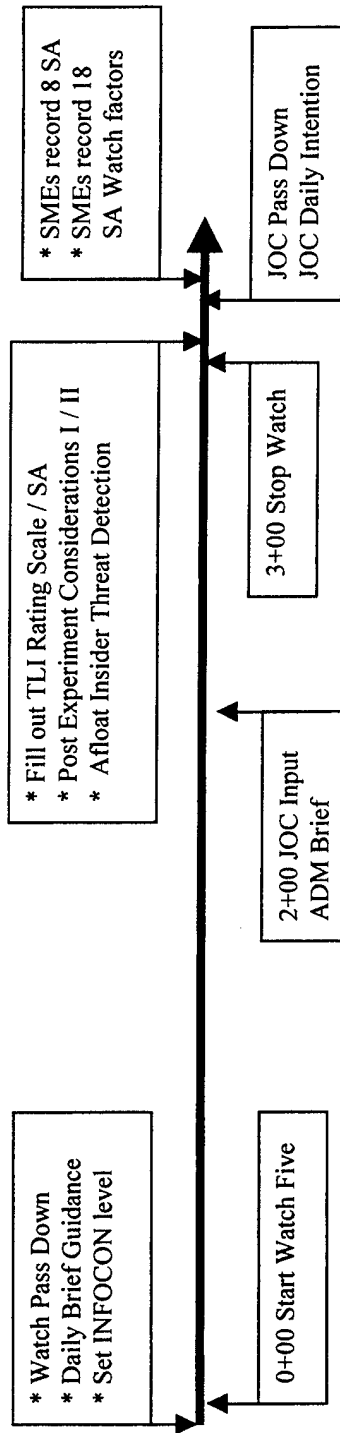
APPENDIX E. IA C2 EXPERIMENT DESIGN AND DATA COLLECTION FLOW



WATCH ONE



Watches Two - Four



Watch Five

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Alberts, D.S., Garstka, J.J., Stein, F.P., "*Network Centric Warfare: Developing and leveraging Information Superiority*," CCRP Publication Series, 1998.
- Cebrowski, Arthur K. VADM, "*Network Centric Warfare: A Revolution in Military Affairs*" Speech, September 1997.
- Chairman Joint Chiefs of Staff, "Joint Vision 2020", [www.dtic.mil/jv2020/jvpub2.htm], February 2000.
- Commander Third Fleet, "INFOCON Standard Operating Procedure", 1 November 1999.
- Computer Science and Telecommunications Board - National Research Council, "*Realizing the Potential of C4I Fundamental Challenges*," National Academy Press, 1999.
- Cook, T.D., Campbell, D.T., *Quasi-Experimentation - Design & Analysis Issues for Field Settings*, Houghton Mifflin Company, 1979.
- Cox, CDR S., Stimeare, MAJ R., Dean, MAJ T., "Information Assurance - the Achilles' Heel of Joint Vision 2010", Armed Forces Staff College, March 1999.
- Critical Infrastructure Assurance Office, *Practices For Securing Critical Information Assets*, January 2000.
- Department of Defense, Chairman, Joint Chiefs of Staff, Memorandum: DoD Information Operation Condition, 31 Dec 1998.
- Department of Defense, Joint Task Force - Computer Network Defense, "INFOCON: Tactics, Techniques and Procedures," 15 November 1999.
- Deputy Secretary of Defense, DoD Memorandum: Information Vulnerability and the World Wide Web, 24 September 1998.
- Galik, CAPT D., "Defense in Depth: Security for Network-Centric Warfare," [http://www.chips.navy.mil/chips/archives/98_apr/Galik.htm], April 1998.
- Gutwin, C., Greenberg, S., "A Framework of Awareness for Small Groups," [<http://www.cpsc.ucalgary.ca/group/lab/papers/1999/99-Awareness Theory/html/theory-tr99-1.html>], 1999.
- Hart, S.G., Staveland, L.E., "*development of NASA-TLX: Results of Empirical and Theoretical Research*," Science Publications, 1988.

Hayden, Lt. Gen M.V., Director, National Security Agency, Address to Kennedy Political Union of American University, 17 February 2000.

Institute for Joint Warfare Analysis, *Complex Experimentation Processes - Fleet Battle Experiment Implementation*, by Schacher G.E., Gallup S.P., January 2001.

Kass, Richard A., "Understanding Joint Warfighting Experiments", USJFOM Joint Experimentation Directorate (J9), 2000.

Mathieson, G.L., Moffat, J., Shirley, D., *A Guide to Best Practice in C2 Assessment*, Defense Evaluation and Research Agency, 1999.

Minihan, Lt. Gen K.A., "U.S. Must Combat Weak Computer Security in Government Information Systems", Prepared statement for Senate Governmental Affairs Committee, Washington, D.C. 24 June 1998.

RAND National Defense Research Institute, *Analytical Methods for Studies and Experiments*, RAND Corporation, Washington D.C., 1999.

SPAWAR Systems Center San Diego, *IA C2 INFOCON Lab Experiment Plan*, by Seymour, G., St Claire, C., 28 April 2000.

Telephone conversation between R. Walker, JIOC J3, and the author, 15 November 2000.

Telephone conversation between Dr. G. Seymour, INFOCON Analyst, SPAWAR Systems Center IOCOF, and the author, 16 February 2001.

Walker, R., "Overview of Information Operations Condition (INFOCON)," *Cyber Sword*, Volume IV, pp. 17-20, April 2000.

Waltz, Edward, *Information Warfare: Principles and Operations*, Artech House, Inc., 1998.

Wilson, Michael, "Defense-in-Depth: Design Notes," 7Pillars Partners, [<http://www.7pillars.com/papers/didfinal.htm>], November 1997.

Vigilant Protector 99-1, INFOCON exercise conducted by SPAWAR Systems Center for COMTHIRDFLT and 1-MEF in Oct 1998 to explore the effects of INFOCON's on the Joint Task Force, October 1998.

Vigilant Protector 99-2, INFOCON exercise conducted by SPAWAR Systems Center for COMCARGRU One in May 1999 to explore the effects of INFOCON's on the Carrier Battle Group, May 1999.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..... 2
8725 John J. Kingman Road, Set. 0944
Fort Beloved, VA 22060-6218

2. Dudley Knox Library..... 2
Naval Postgraduate School
411 Dyer Road
Monterey, California 93943-5101

3. Professor William G. Kemple 1
Code JW
Naval Postgraduate School
Monterey, CA 93943

4. Professor Shelley P. Gallup 1
Code JW
Naval Postgraduate School
Monterey, CA 93943

5. Mr. Richard A. Kimmel..... 6
Code JW
Naval Postgraduate School
Monterey, CA 93943