STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DEVELOPING AND RETAINING INFORMATION WARRIORS: AN IMPERATIVE TO ACHIEVE INFORMATION SUPERIORITY

BY

LIEUTENANT COLONEL RUSSELL F. MILLER
United States Air Force

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2000

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

20000526 053

DTIC QUALITY INSPECTED 3

USAWC STRATEGY RESEARCH PROJECT

DEVELOPING AND RETAINING INFORMATION WARRIORS: AN IMPERATIVE TO ACHIEVE INFORMATION SUPERIORITY

by

LIEUTENANT COLONEL RUSSELL F. MILLER
United States Air Force

Colonel Ralph D. Ghent
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

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

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: Russell F. Miller, LTC, United States Air Force

TITLE: Developing and Retaining Information Warriors: An Imperative to Achieve Information Superiority

FORMAT: Strategy Research Project

DATE: 29 February 2000 PAGES: 37 CLASSIFICATION: Unclassified

Developing effective policy, doctrine, organizations, technology, and most importantly, skilled people are essential to ensure our warfighters enjoy information superiority across the spectrum of conflict. In this context, "information warriors"–people skilled in the art of conducting information operations–are essential to achieving information superiority. Information warriors must be multi-skilled—at a minimum, proficient in operations, intelligence and information technologies. Unfortunately, all military services face significant challenges in retaining information technology (IT) professionals—people with many of the critical skills needed to conduct effective information operations. This paper analyzes Air Force IT retention and its impact on achieving information superiority. In this context, information superiority is the desirable end-state, information operations the way to win it, and standing up a new Air Force Information Operations (IO) career field the best way to retain the IT professionals needed to achieve it. Key reasons IT professionals leave the Air Force are identified, leading to the conclusion that to improve IT retention, the Air Force must do a better job addressing both tangible and non-tangible satisfiers. Besides aiding IT retention, a separate Air Force IO career track is the best way to develop "information warriors"—the people warfighters will task to win information superiority on future battlefields. Joint Vision 2010 makes it clear that attracting and retaining people with the intellect, training and motivation to prevail across the spectrum of military operations is critical to the future success of our forces. To that end, developing and retaining "information warriors" capable of conducting decisive information operations is a strategic, operational and tactical imperative. To fail in this endeavor will significantly jeopardize our ability to prevail in future conflicts.

TABLE OF CONTENTS

ABSTRACT iii

LIST OF ILLUSTRATIONS vii

DEVELOPING AND RETAINING INFORMATION WARRIORS: AN IMPERATIVE TO ACHIEVE INFORMATION SUPERIORITY 1

INFORMATION SUPERIORITY...AN OPERATIONAL IMPERATIVE 2

THREATS TO ACHIEVING INFORMATION SUPERIORITY 4

INFORMATION OPERATIONS—THE WAY TO ACHIEVE INFORMATION SUPERIORITY 6

WHAT SKILLS ARE NEEDED TO CONDUCT IO? 6

WHY ARE IT PROFESSIONALS LEAVING THE AIR FORCE? 9

THE CASE FOR AN AF IO CAREER FIELD 15

AN AIR FORCE IO CAREER FIELD—CHARACTERISTICS, STRUCTURE, BENEFITS 18

A NOTIONAL AIR FORCE IO OFFICER CAREER PATH 19

BENEFITS OF AN AIR FORCE IO CAREER FIELD 20

CONCLUSION 22

ENDNOTES 23

BIBLIOGRAPHY 27

LIST OF ILLUSTRATIONS

FIGURE 1. IO CAPABILITIES AND RELATED ACTIVITIES FROM JP 3-13 7

FIGURE 2. IO CELL FROM JP 3-13 7

FIGURE 3. ENLISTED COMM-COMPUTER SYSTEMS OPERATOR MANNING 11

FIGURE 4. COMMUNICATIONS AND INFORMATION OFFICER MANNING 11

DEVELOPING AND RETAINING INFORMATION WARRIORS: AN IMPERATIVE TO ACHIEVE INFORMATION SUPERIORITY

> Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.[1]
>
> —Air Marshall Guilio Douhet

Achieving information superiority is an essential prerequisite for success on 21st Century battlefields. However, to achieve information superiority, the military services must build the proper framework. Effective policy, doctrine, organizations, technology, and most importantly, skilled people are all needed to ensure our warfighters enjoy information superiority across the spectrum of conflict. In this context, the people tasked to achieve information superiority must be skilled in the art of conducting information operations—people referred to in this paper as "information warriors." Information warriors must be multi-skilled—at the very least schooled in operations, intelligence and information technology.

Unfortunately, all the military services face significant challenges in retaining information technology (IT) professionals—people with many of the skills required to conduct effective information operations. There are many reasons for these defections: inadequate compensation, high PERSTEMPO, and industry competition are just a few–but they don't tell the whole story. A host of intellectual, perceptual, and emotional factors are at work too. Consequently, for the services to successfully retain IT professionals, they must do a better job addressing both tangible and intangible satisfiers.

This paper analyzes Air Force IT retention and its impact on achieving information superiority. In this context, information superiority is the desirable end-state, information operations the way to win it, and standing up a new Air Force Information Operations (IO) career field the best way to retain the IT professionals needed to achieve it. Addressing the following pertinent questions facilitate the analysis: Why is information superiority important and what are the threats to achieving it? What does IO have to do with information superiority? What skills are needed to conduct IO? Why are IT professionals leaving the Air Force and why does it matter? How can the Air Force retain its IT professionals?

My analysis will logically lead to the recommendation to implement an IO career field to develop Air Force "information warriors." This new career field is envisioned--not only as the best way to conduct information operations--but also as an essential step the Air Force must take to train and retain IT professionals. This recommendation also includes a suggestion on how this new IO career field could be structured. Information superiority is essential to conducting effective joint and aerospace operations. Thus, developing and retaining information warriors is an Air Force strategic, operational and tactical imperative. Standing up an Air Force IO career field is the right thing to do—and now is the right time to do it!

INFORMATION SUPERIORITY...AN OPERATIONAL IMPERATIVE

We must have information superiority.[2]

—Joint Vision 2010

Joint Vision 2010 (JV 2010) emphasizes the importance of achieving information superiority--the capability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same—as the critical prerequisite to achieving military success in the 21st Century. Indeed, JV 2010 characterizes information superiority as the essential enabler for all our emerging operational concepts: dominant maneuver, precision engagement, focused logistics and full dimensional protection.[3] Dominant battlespace awareness, improved weapons lethality, the ability to mass effects vice the need to mass forces, and the ability to rapidly adapt to an increasingly lethal battlespace are all critical tasks enabled by achieving information superiority. While enabling breakthrough operational capabilities for combat forces, information technology also enhances combat support effectiveness. As a result, the military services are increasingly dependent on information technology to achieve their day-to-day missions of training, organizing, and equipping their forces.

The pressures to downsize the military after the cold war sparked an increased demand for information technology as a way to leverage the efficiencies of computers, computer networks and information systems against the need for people. As a result, there is not one functional area—operations, intelligence, weather, communications, engineering, logistics, services, security, etc. that doesn't rely extensively on information systems to get their day-to-day jobs done. While information systems have generally made processes more efficient, one unintended consequence is there is no longer enough people to get the job done if these information systems fail. As an example, compare shopping in yesterday's stores using manual cash registers to today's use of computerized checkouts. When the power failed, yesterday's stores still conducted business because they had the people and technology to do so. Today, when the power fails, stores must close because they've become dependent on technology--for pricing information, credit checks, real-time inventory control etc.—and no longer have the people or systems to conduct business any other way. This analogy also applies across the military services. All functional areas rely on information networks and systems to conduct daily operations in peace and war. Given today's austere resource environment, it appears there's no going back. For good or bad, our reliance on technology makes information systems one of our strategic and operational centers of gravity.

The military's reliance on information technology (IT) is a mixed blessing. Not only has it increased our operational capabilities, it has also increased our vulnerabilities. The information-based systems that were key to our overwhelming success in Desert Storm are even more critical to executing combat operations and delivering effective combat support today. But this technological strength also represents our Achilles heel. Information systems are now so imbedded in the way we fight, protecting them has become the sine-qua-non for military success. And to the extent our adversaries rely on them too, our

ability to attack enemy information infrastructures will impact our ability to prevail in any future conflict. Winning information superiority and enjoying all the strategic, operational and tactical benefits it delivers will not be an uncontested battle. We face real external and internal threats to achieve information superiority—threats made even more challenging because they are constantly changing.

THREATS TO ACHIEVING INFORMATION SUPERIORITY

> We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers.[4]
>
> —John M. Deutsch, Director, CIA
> Washington Post, 26 June 1996.

External threats to our information infrastructure could come from a future peer competitor. According to the Washington Times, quoting an article published in the official daily newspaper of China's People Liberation Army, China is considering developing a fourth branch of their armed services to conduct information warfare over the Internet.[5] This news not only raised concerns in the Pentagon over China's potential threat to U.S. communications, transportation, finance, and electrical power networks, but also initiated concerns over our military's dominance in high-technology weapons and war fighting.[6] Indeed, Vice Admiral Thomas Wilson, the new director of the Defense Intelligence Agency indicated that China's announced plan to conduct "Internet Warfare" poses a threat to U.S. military dominance on the battlefield because the United States and the Pentagon are very "information dependent."[7]

External threats, however, aren't confined to potential peer competitors. The threat of asymmetric attacks to our information systems by individuals, non-state actors or terrorist groups is very real. In fact, one of the most troublesome challenges confronting our information-dependent military forces is that any future adversary could gain a quantum leap in their military capabilities by acquiring information technology readily available in the market place which could easily counter U.S. military strengths.[8] During Eligible Receiver, a U.S. military exercise conducted in 1997, a young lieutenant using an ordinary computer and modem successfully broke into the Pacific Fleet's command and control network, masqueraded as the fleet commander and issued bogus movement orders which the fleet followed![9] In this case, a team of "friendly" hackers was employed in the exercise to demonstrate how individuals could compromise military information systems using computers, modems and software technology widely available on the Internet.[10] However, this example raised concerns beyond the mischief possible by individual hackers. Eligible Receiver highlighted the more pernicious damage a malevolent non-state actor or terrorist group could inflict on our information-system-dependent military forces with a small investment in readily available technology. Future enemies understand our reliance on information technology and will certainly learn how to nullify our advantage. As DoD pointed out in its 1999 Annual Report, "Those who oppose the United States will increasingly rely on unconventional strategies and tactics to offset U.S. superiority in conventional forces. The Department's ability to adapt effectively to adversaries' asymmetric threats—such as information operations—is critical to maintaining U.S. preeminence into the next century."[11] While the external threats to achieving information superiority are challenging, they aren't the only threats the Air Force faces in trying to achieve information superiority.

Besides external information attacks which could deny critical services or spoof our information systems, there are many internal threats to achieving information superiority. One serious internal threat involves the adverse impact inadequately trained IT professionals have on the security and reliability of our networks. According to statistics from Air Combat Command (ACC), in 1998, the majority of network service disruptions were not caused by hackers. Instead, they occurred from self-inflicted errors, unintentionally introduced by network maintainers—IT professionals--responsible for making software changes. In one incident, an outage induced by a system administrator at Minot Air Force Base, North Dakota while updating his server's public access folders caused an ACC-wide Internet access outage that lasted three days. Operator error is often the cause of an increasing number of network failures.[12]

These types of training shortfalls were previously identified by a Defense Science Board Task Force study which found significant DoD information system vulnerabilities resulting from "human error, insufficient training, or lack of knowledge."[13] The Task Force also found that the capabilities of system and network administrators and system managers varied widely.[14] Among the Task Force's many recommendations to fix the shortfalls they found was this one: "To staff for success, a cadre of high-quality, trained professionals with recognized career paths is an essential ingredient for defending present and future information systems—not people tasked with other duties as assigned."[15] Directly contributing to this training problem is the challenge all military services have retaining information technology (IT) professionals. IT retention is examined in detail later in this paper.

As if coping with these external and internal threats wasn't enough, achieving information superiority is made even more difficult because the nature of the threats is rapidly changing. Apparently, having the "capability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same" is not the entire prescription for achieving information superiority. A new form of information conflict is emerging that suggests an entirely new set of principles governs the realm of information conflict—netwar. Netwar is based on a strategy that involves accessing a network—not to destroy it or deny its use—but to use it as a tool to gather support and maintain communication.[16] Currently, many terrorist and criminal groups, to include Osama bin Laden and his Al Quaeda organization, use netwar to enhance the cohesion of their group and to execute their agenda by getting their message on the internet to facilitate a "war of ideas to manage international perceptions." [17] Air Force doctrine now recognizes two different aspects of information superiority: information warfare and information-in-warfare.[18] Clearly, the type, nature and scope of these potential threats to achieving information superiority present complex challenges that stress cold war legacy operational doctrine, organizations, and training. Given this challenging, dynamic environment, how will we develop people with all the requisite skills to achieve information superiority? Establishing the relationship between information superiority, information operations and information warfare will lay the needed foundation to answer that question.

INFORMATION OPERATIONS—THE WAY TO ACHIEVE INFORMATION SUPERIORITY

> For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.[19]
>
> —Sun Tzu

Two key terms—defined in Joint Publication 3-13 (JP 3-13), Joint Doctrine for Information Operations–relate the concept of information superiority to the actions necessary to achieve it. The first term is information operations (IO), defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[20] The second term is information warfare (IW), defined as "information operations conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries."[21] IO is further divided into two major subdivisions: offensive IO and defensive IO. Offensive IO involves integrated activities to affect adversary decision-makers. Defensive IO involves the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems.[22]

Responsibility to conduct IO is not the exclusive domain of any one service or unified command nor could it be. IO must be an essential capability of all military organizations to conduct effective operations from peacetime theater engagement to high intensity combat.[23] Perhaps less intuitive is that within the Joint Staff, IO responsibilities are split with the J-3 responsible for offensive IO and the J-6 responsible for defensive IO. In addition, the aggregate skills needed to conduct offensive and defensive IO do not reside in any one Air Force military or civilian specialty. As we will now discuss, these facts of life complicate forming organizations and developing effective processes to develop and execute a Joint Force Commander's (JFC) IO campaign.

WHAT SKILLS ARE NEEDED TO CONDUCT IO?

> Only the most dedicated, well-trained personnel with first class leaders will succeed in the complex and fast-paced environment of future military operations.[24]
>
> —General Shalikashvili, 1997 National Military Strategy

By definition and practice, Information Operations are complex actions whose successful planning and execution demand the smart integration of many different skills and many different specialties: operations, intelligence and information technology. In fact, conducting effective IO requires integrating the many capabilities and related activities depicted in Figure 1.

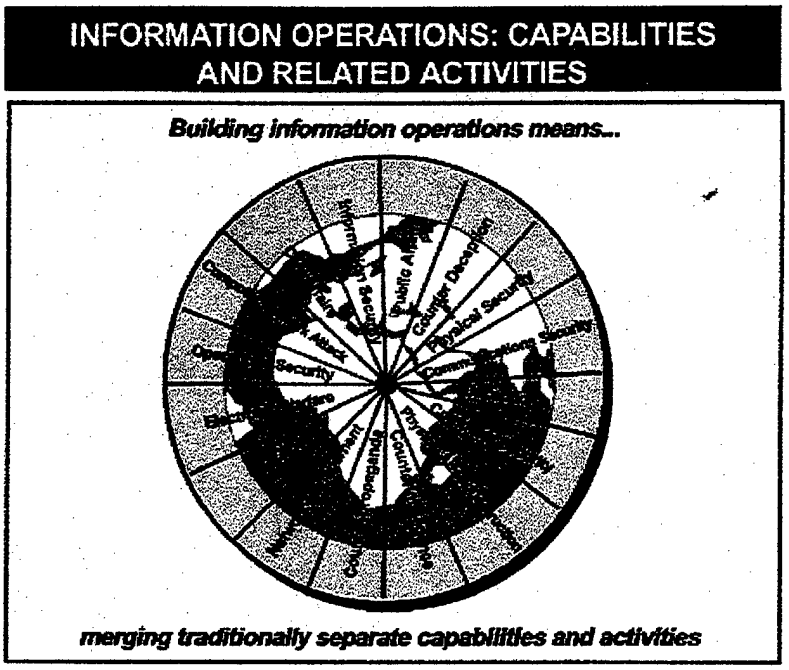


FIGURE 1. IO CAPABILITIES AND RELATED ACTIVITIES FROM JP 3-13[25]

In joint operations, the organization tasked to produce a warfighter's integrated IO plan is the IO cell. The structure and composition of a fully functional IO cell is shown in Figure 2. Doctrinally, in a Joint Task Force (JTF) the JFC's staff, along with the IO cell, develops the IO guidance and plans that are passed down to the components, supporting organizations and agencies for detailed mission planning.

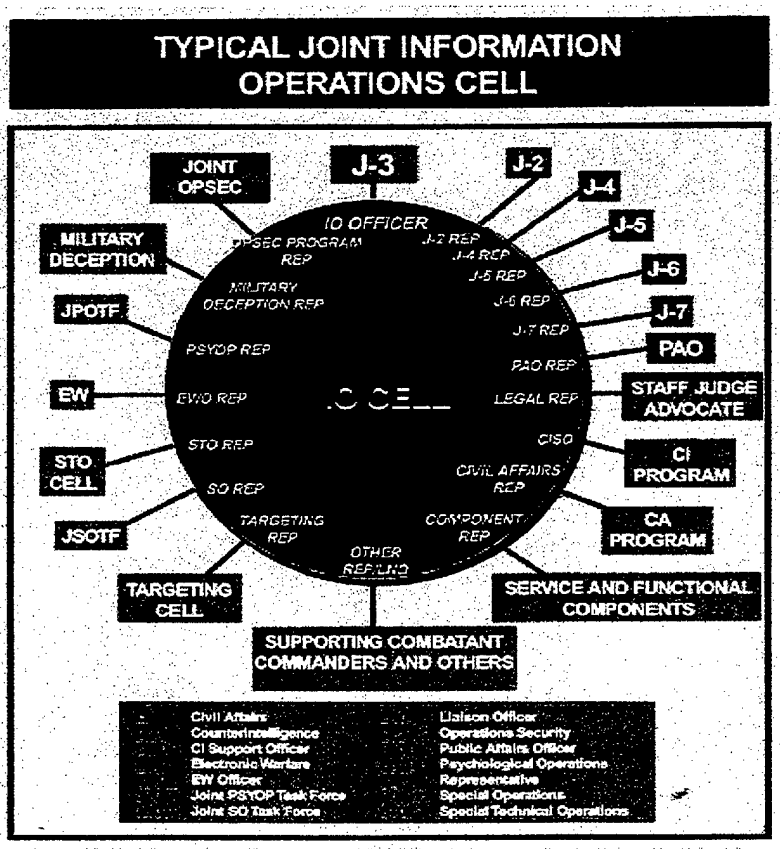


FIGURE 2. IO CELL FROM JP 3-13[26]

There's only one problem with current joint IO doctrine—it doesn't work. Experiences during Operation ALLIED FORCE revealed significant doctrinal shortfalls. According to the lead "surrogate" IO planner on the JCS/J-39 staff, there were three difficulties that kept the JFC's staff from developing its own IO plan as mandated by JP 3-13. First, the U.S. European Command (USEUCOM) and JFC staffs were busy working time-sensitive deployment and operational issues—tasks that precluded their participation in a separate IO cell which competed for many of the same people. Second, the resulting IO plan required coordination and approval well above the USEUCOM staff, and as it turned out, outside of DoD. Third, and most insightful, operational planners didn't think an IO cell (as conceived in JP 3-13) could develop an effective IO campaign given the lack of IO expertise on the USEUCOM and JFC's staffs. Their assessment was that it was too hard for a matrixed staff comprised of many "stove-piped" disciplines to put together an effective IO campaign—a plan with the necessary degree of integration required to accomplish the JFC's strategic, operational, and tactical objectives. As a consequence, it fell to the JCS/J-39 staff to pull together a small cadre of the very few IO experts in DoD to develop, coordinate, and win approval of the IO campaign executed in Kosovo.[27]

In sum, the organizations and skills needed to do efficient IO planning and coordination for Operation ALLIED FORCE exceeded the capabilities of the warfighter's staff. What's needed is a cadre of "information warriors"—experts who have all the operational and technical skills required to plan and execute successful information operations. People with the right amalgam of skills would also help create much simpler staff organizations, vice the myriad people now needed to develop an IO campaign. This problem begs for a fix; however, it's not just a joint problem. Per joint doctrine, service components must also have the capability to plan and execute IO on short notice immediately upon arrival in an operational area.[28] While Air Force efforts will focus on implementing IO capabilities in support of joint warfighting commands, the Air Force's Aerospace Expeditionary Force (AEF) must be ready to perform theater-level strategic, operational, and tactical information warfare.[29]

The Air Force must be ready to conduct effective IO in the 21st Century. Future aerospace superiority will depend on superior battlespace awareness--an important product delivered by information networks. Unfortunately, there's a fly in the ointment. Air Force IT professionals, Communications and Information (C&I) officers, Air Force Specialty Code (AFSC) 33S and enlisted Communications-Computer Systems Operators, AFSC 3C0X1—the people who provide and protect Air Force networks—are leaving active duty in record numbers. We must understand why they're leaving so we know what to fix and how to fix it.

WHY ARE IT PROFESSIONALS LEAVING THE AIR FORCE?

> We will have to say that in any cause the decisive role does not belong to technology—behind technology there is always a living person without whom technology is dead.[30]
>
> —Mikhail Frunze, quoted in Gareyev, Frunze, Military Theorist, 1985

All military services have serious retention problems. In fact, in FY99, the Air Force missed their retention goals in all three categories of first term, second term and career airman.[31] Unfortunately, none of the four services conduct formal exit interviews to determine the root causes for enlisted separations. However in one study, DoD interviewed 254 separating first term enlistees to determine why they were leaving. The most frequently cited reasons mentioned were quality of life concerns: the perceived erosion of benefits, pay, and advancement opportunities, coupled with long work hours and frequent deployments. Many felt military retirement and medical benefits were eroding and their salaries were not competitive with the private sector. Interestingly, the people who believed they could make more money in the private sector were those in military specialties with highly transferable technical skills, such as those who worked with computers.[32]

Those dissatisfied with the military's quality of life provide a willing ear to an increasingly aggressive civilian job market that competes for skilled military labor. Low unemployment, coupled with low inflation (the best in 30 years) has resulted in unprecedented economic conditions in America.[33] While a growing national economy isn't the reason people leave military service, it certainly enables people to leave. With the economy in such good shape, military job security is no longer considered a major benefit. In this environment, civilian corporations actively compete with the military for talent to staff America's labor force. As General Patrick Gamble, Pacific Air Forces Commander pointed out, "Retention is tough for the Air Force because our high-quality people are highly sought by non-military employers. Businesses love to recruit people from us—our people are honest, hard-working, committed and loyal."[34] And nowhere is this competition with industry stronger than it is for IT professionals.

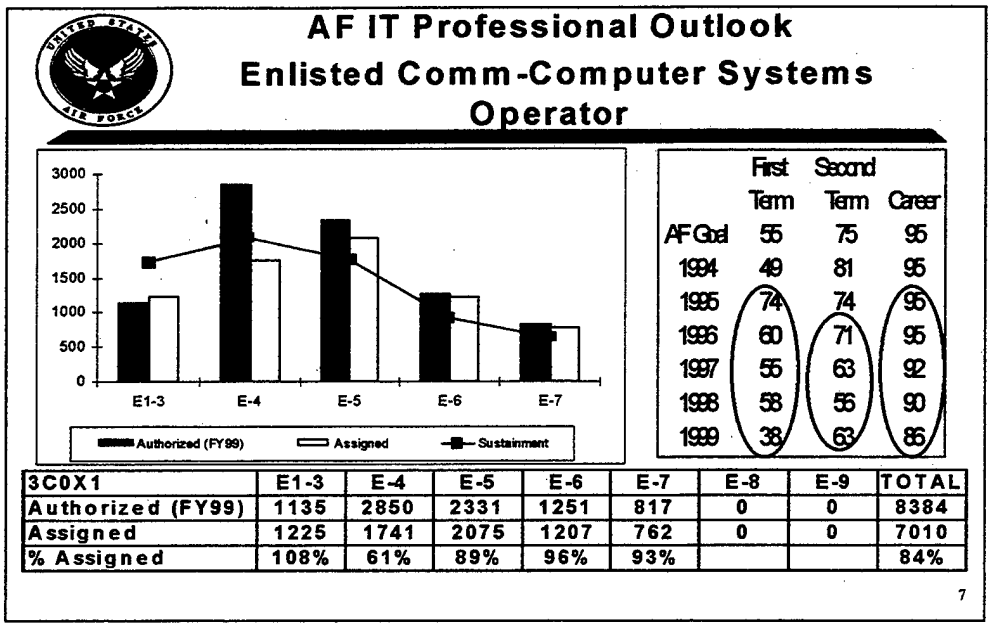
The problem of finding and keeping an adequate number of IT professionals is a growing worldwide dilemma. In the U.S., industries cannot keep up with the demand for new information technology workers. A survey of mid- and large-size U.S. companies by the Information Technology Association of America (ITAA) concluded that at the time of their survey, there were about 346,000 unfilled information technology jobs in the United States due to a shortage of qualified workers.[35] A U.S. Department of Commerce study observed that half the CEOs of America's fastest growing companies reported an inadequate number of information technology workers to staff their operations.[36] The study further reported growing "evidence that job growth in information technology fields now exceeds the production of talent."[37] In another study by the Stanford Computer Industry Project, researchers found a worldwide shortage of IT workers.[38] A survey of some 1,500 chief information officers (CIOs) in 21

countries, indicated IT managers throughout the world are experiencing unprecedented demand for IT workers and high turnover rates.[39] The demand for IT professionals appears insatiable.

Considering the shortage of IT workers in the global labor pool, the military services face tough competition with the public and private sectors as they seek to satisfy their own rapidly expanding IT needs. The competition for talent is evident in the market place by observing the increasing salaries and benefits that industry is offering to attract and retain skilled IT workers. A compensation survey conducted by William M. Mercer showed that average hourly compensation for operating systems/software architects and consultants rose nearly 20 percent from 1995 to 1996.[40] Another survey conducted by the Deloitte & Touche Consulting Group revealed that salaries for computer network professionals rose an average of 7.4 percent from 1996 to 1997.[41] Besides salary increases, significant hiring bonuses, Employee Stock Option Plans (ESOP) and portable 401(k) retirement plans are used extensively to attract and keep top IT talent.[42] In this game, the military finds it difficult to compete. Why stay in when less demanding, better-paying jobs are available on the outside?

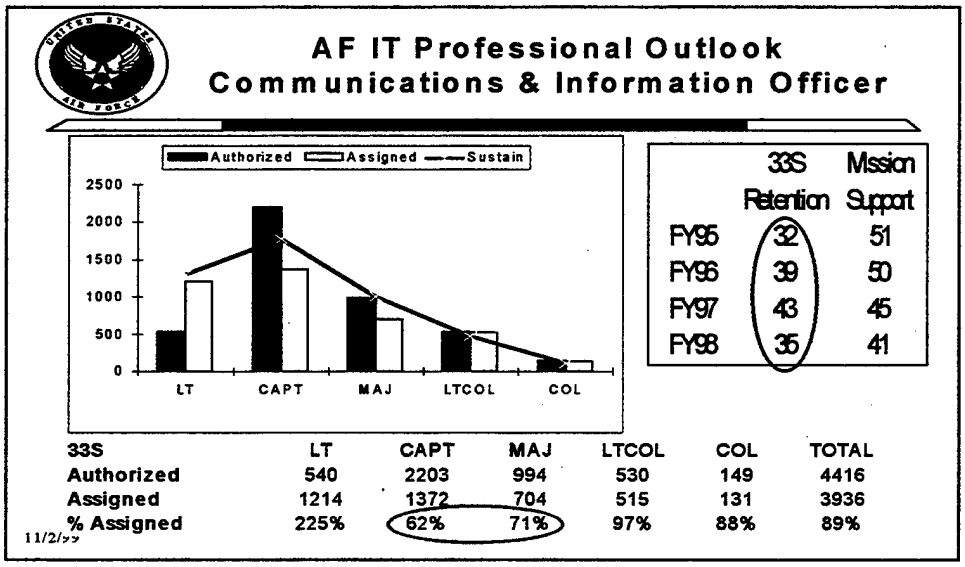
All military services face significant challenges in retaining information technology (IT) professionals—especially people currently tasked with providing and protecting the networks that serve as the information highways for our combat and combat support forces. While symptomatic of the larger problems the services have in recruiting and retaining military personnel, the challenges of retaining IT professionals is particularly troublesome and is attracting the attention of senior leadership across the services. For example, the Commanding General, U.S. Army Europe expressed concern over the qualifications and retention of the soldiers he has maintaining his information networks. In an E-mail to the Vice Chief of Staff of the Army, he stated, "Need to put a program together to train and develop the cadre who will be the master gunners of the info age for the Army. Need standards...professional development...financial incentives to keep those we train. Many will say we don't have the money to do this. By a factor of 100, we don't have the money to repair the damage if we don't."[43] This commander understands that you can't achieve information superiority with technology alone. Along with "smart boxes," you need smart people—the "master gunners" of the information age. Training and retaining IT personnel is an acute problem in the Air Force too.

Retention of Air Force enlisted 3C0X1s has decreased markedly since 1995 with dramatic downturns in Fiscal Years 97 and 98 (Figure 3). While not as critical as the AF's pilot problem, retention, of 33S officers lags significantly behind other mission support specialties like security police, personnel, and civil engineering (Figure 4). Many Air Force IT professionals leave the service for the same reasons other military professionals leave--civilian-military pay disparities, inadequate military housing, and concerns over diminishing health and retirement benefits are among the main dissatisfiers.[44] However, intrinsic concerns are not the only reasons Air Force IT professionals leave active duty. Job satisfaction—which includes a host of non-tangible, psychological factors—increasingly determines whether IT professionals, inside and outside of the military, stay or leave their current job.



3C0X1	E1-3	E-4	E-5	E-6	E-7	E-8	E-9	TOTAL
Authorized (FY99)	1135	2850	2331	1251	817	0	0	8384
Assigned	1225	1741	2075	1207	762	0	0	7010
% Assigned	108%	61%	89%	96%	93%			84%

FIGURE 3. ENLISTED COMM-COMPUTER SYSTEMS OPERATOR MANNING[45]



33S	LT	CAPT	MAJ	LTCOL	COL	TOTAL
Authorized	540	2203	994	530	149	4416
Assigned	1214	1372	704	515	131	3936
% Assigned	225%	62%	71%	97%	88%	89%

FIGURE 4. COMMUNICATIONS AND INFORMATION OFFICER MANNING[46]

Many studies by government and non-government agencies indicate IT professionals are not just motivated by money. Besides salary, bonuses and benefits, studies emphasize that psychological factors increasingly motivate IT workers to either stay or leave their jobs. This relationship was summed up succinctly by Lawrence J. Delaney, Assistant Secretary of the Air Force (Acquisition): Retention = Monetary Compensation + Psychological Compensation, or R = MC + PC.[47] These non-intrinsic, psychological factors are relevant to IT workers in the public and private sectors, inside and outside of

government.[48] These findings are not surprising; they are entirely consistent with classic motivational theories proposed many years ago by Abraham H. Maslow and Frederick Herzberg.

Maslow's hierarchy of needs proposed that man was motivated by his physiological needs first, and only after his physical needs were satisfied would he try to satisfy higher level needs: safety, social, ego and at the top, self-actualization.[49] Herzberg's theory of motivation postulates that man has two fundamental needs: to avoid dissatisfaction and to seek satisfaction. Further, satisfaction and dissatisfaction are two separate attitudes, each with a different set of goals and needs. Factors that lead to job satisfaction are termed "motivators" because they reward the need for psychological growth.[50] These theories provide a solid underpinning to help us better understand psychological factors that affect IT retention.

These theories predict that once lower level needs are satisfied, higher level needs predominate. The 4.8% pay raise, the largest since 1982, and repeal of the Redux--restoring the 20-year retirement plan with 50% base pay and full cost of living allowance--were major accomplishments in FY00 that helped satisfy the physiological and security needs of most military members. However, with these fundamental needs satisfied, higher level needs--like quality of life—increasingly drive the needs of service members. For IT professionals, these quality of life concerns include a host of non-tangible "motivators" that seek to reward the need for psychological growth and job satisfaction. So what are the psychological factors affecting IT job satisfaction?

Over the years, many aspects of the Air Force's IT work environment have negatively impacted IT job satisfaction--issues this author became acutely aware of as commander of two communications squadrons from 1993 to 1995 and 1997 to 1999. These factors influence the attitudes and morale of Air Force communicators and their retention decisions in an environment of growing private sector competition.

A major IT workforce study conducted by the Army confirmed that psychological (motivational) compensation issues were essential to building a highly motivated IT workforce. High on the list of psychological satisfiers was training.[51] This also tracks with an earlier survey conducted by *Information Week* that found training "the number one technique used by IT managers to attract and retain IT professionals."[52] The authoritative Gartner Group also reported "training is a big part of the IT retention issue."[53] Also high on the list was achievement, the opportunity to earn technical certifications by mastering new technology, performing interesting and challenging work, opportunities for continuous learning, and working in an organization that delegates responsibility to manage and lead projects.[54]

Unfortunately, training is one of the major dissatisfiers for many Air Force IT professionals, particularly for new systems they're asked to maintain. As one senior Air Force communications career field manager observed, "Many times Air Force communicators are tasked to take care of new systems because there was not enough money to pay for contract maintenance. The problem is they never get trained on these systems which causes a lot of frustration. Training is a big problem."[55] Absent adequate

training, many organizations must use their own funds to train IT workers. However in an ironic "Catch-22," their initiative often backfires. Since no additional active duty service commitments (ADSC) are incurred for local training, the Air Force rarely gets an adequate return on its investment. Further, the training often makes IT professionals more competitive for jobs on the outside.

Besides training, another major dissatisfier affecting Air Force communicators is the effort to downsize communications career fields through Competitive Sourcing and Privatization (CS&P). These continuing initiatives, started in 1996, target almost all base-level communications and information functions. The scope of the effort varies depending on the Major Command; however they foster an almost universal attitude among Air Force communicators: The Air Force no longer has a job for me; they're giving them to contractors and Air Force civilians. While major savings were accrued by outsourcing non-military essential information services, the adverse impact of CS&P on the morale of Air Force communicators cannot be overstated. People who joined the Air Force to work with information technology are now asked to stay in and be contract monitors or quality assurance evaluators, work they consider boring and far less challenging. For many, military IT jobs in the Air Force are disappearing while employment opportunities on the outside are abundant. If "bluesuit" IT providers aren't cost effective, the AF must determine what military-essential business they should be in.

Another dissatisfier involves what some Air Force communicators describe as having to work for technologically-challenged, "Dilbert-like" bosses who do not understand what IT professionals do and don't seem to value them. Sometimes these bosses over-commit their IT workforce—tasking them with more and more work without adequate resources. In particular, the manpower to take care of the base network has not kept pace with all the functional systems using it. Consequently, many IT professionals work long hours, and even when they are off duty, must still respond to after-hour network outages. Sometimes these bosses impose unreasonable demands to deliver IT services in a compressed time frame without additional resources. These contests often create a tense, confrontational environment most IT professionals would rather avoid. As young officers are quick to observe, when the role of IT is misunderstood, the wing IT leader's contribution is usually not valued either. As these officers then consider growing up in this environment, many conclude it's not worth it.

Other frustrations that affect the job satisfaction of IT professionals include an environment where customers do not value the IT services they provide. Unfortunately, in some wing's IT is only considered an administrative utility, of little value to the wing's operational mission. By way of contrast, IT and IT professionals in industry are considered important, strategic, competitive assets. Other IT professionals are frustrated by how slowly the military implements new technology. On the other hand, they view industry as being committed to rapidly employ technology to maintain competitive advantage. And finally, many Air Force IT professionals are dissatisfied by a lack of opportunities to grow. Network maintainers express frustration at being "stovepiped" in their jobs because they are in "critical one deep" positions and considered too valuable to lose for training or to gain experience in another job. Conversely, in industry the sheer size of the private sector seems to guarantee a better opportunity for competitive advancement.

Given all these dissatisfiers, one could easily conclude that the IT retention problem is too hard to fix. Maybe it is. However, there may be a glimmer of hope for the military in its competition with industry for IT professionals. Despite the appeal of the private sector, many IT professionals still choose to stay in the military. Why they stay in is more instructive than why they leave.

General Donahue, the Air Force's top communicator put the IT retention challenge and relationship of tangible and non-tangible satisfiers into perspective when he remarked, "Any high performing organization works recruiting and retention hard and when there is intense competition worldwide for the skills you'd better pay attention to this. The issue of scarce IT talent is a national issue and we are not going to get into a bidding war with the private sector. We want people who want to serve, who want responsibility and opportunity to do things you just can't do in the private sector. We will adequately compensate them and we will take care of their families. People stay with us who have had success in operationally relevant jobs on important missions."[56] General Donald Peterson, Air Force Deputy Chief of Staff for Personnel, also echoed the need to find the proper balance of incentives; "Our task is complex. We must find the appropriate mix of tangible and intangible factors. These intangibles include teamwork, camaraderie, and high quality of people in the Air Force and the satisfaction of serving our nation."[57] These comments reveal a growing realization that previous attempts to "buy" a professional force have not worked. Other compelling, "intangible" factors—patriotism, job satisfaction, and the chance to be a warrior—are also key.

The value of non-tangible motivators is resonating across the services. Michael Gravens, chief, sergeant major in the Fourth Infantry Division at Fort Hood, Texas – the Army's prototype digitized division – said the Army "cannot compete with the commercial world" in terms of salaries, but the Army manages to retain dedicated IT soldiers who view their careers as more than just a way to get a paycheck. The Army still can tap into personnel who willingly forsake the big dollars for love of country and love of the Army."[58] Reinforcing these sentiments, Maj. Charles Wells, who works in the Army's strategic and advanced computing center in the Pentagon, said that "maybe we shouldn't even try to compete with commercial enterprises. The challenge of a military career provides more than compensation. I'm using my skills in a challenging real-world environment. I'm only a junior officer, but I'm building the Army's intranet."[59]

Apparently, the task to retain IT professionals, while difficult, is not impossible. So what should we do? General Donahue has the answer: "We need to make sure our specialties, training, career opportunities are relevant to Air Force needs."[60] In this context, the Air Force needs to stand up a separate Information Operations career field—a new specialty to develop people with all the skills needed to conduct information operations and deliver information superiority on future battlefields. Not surprisingly, standing up an IO career field also promises to help retain IT professionals.

THE CASE FOR AN AF IO CAREER FIELD

> Our education and training programs must prepare joint warriors to meet the challenges of the future battlespace. These programs must emphasize employment of new technologies and achieving the operational concepts outlined in this vision.[61]
>
> —JV 2010

The Air Force's current plan for developing "information warriors" to conduct IO is still evolving and has yet to address some significant shortcomings. While most leaders recognize the need for an information warrior—an operator equipped with all the skills needed to plan and execute the full range of IO–differences exist across the various Air Force functional communities on how to get there from here. One approach is the Information Operations Integration Course (IOIC), developed by the USAF Air Intelligence Agency (AIA) and taught by the 39th Intelligence Operations Squadron at Hurlburt Field, FL. Currently this course is the only USAF education and training program that addresses the entirety of IO and is designed for an annual throughput of 75 students. The first IOIC class was held for 69 academic days, 25 Oct 99 to 14 Feb 00. The IOIC takes experienced officers and enlisted personnel, from the intelligence, communications, special investigations, operations and scientific communities, and teaches them IO planning and execution skills. Common and specialized blocks of instruction are followed by a series of practical exercises. IOIC graduates will be assigned to IW Flights (IWFs), supporting operational Numbered Air Forces (NAFs) or Major Commands (MAJCOMS). Graduates of the IOIC are classified and tracked within the Air Force personnel system. Those holding eligible Air Force Specialty Codes (AFSCs), are authorized a "U" Prefix to their AFSC, after accumulating 12 months experience in an IO position.

In the recent past, the Air Force employed a single Information Warfare Squadron (IWS) primarily focused on Defensive Counter Information (DCI) operations that included activities to defend friendly information and information systems. Today, IW capabilities for the Commander, Air Force Forces (COMAFFOR) are provided by IWFs, owned and operated by the Numbered Air Forces (NAF). During times of crisis, IWFs form the core of the Joint Forces Air Component Commander (JFACC) Air Operations Center (AOC) or Joint Task Force IO cells to plan, coordinate and execute offensive and defensive IO. These IW organizations are tasked to ensure all air component key sensors, weapon systems, and dissemination systems are not degraded by an attack on critical information or information systems. Possible tasks in reaction to a tactical system's attack includes counterattack (by physical or technical means), containment, or feeding the attacker false information (for example, deception). Specific duties may include operational tactics, analysis, and maintenance of support DCI data bases, assisting in the recovery of attacked systems, performing in-theater security assessments, evaluating defensive capabilities, and identifying vulnerabilities by providing tactical warning and attack assessment.[62]

Another approach to make IO warriors was developed at the USAF Weapons School whose mission is to provide the world's most advanced training in weapons and tactics employment to officers of

the combat air forces. They proposed standing up a Communications and Information Weapons School to "close the gap between the communications and information career (C&I) field and the skills required by information warriors."[63] What was missing according to them was that the C&I career field trained to a technical skill set but did not train C&I professionals on campaign planning and weapons employment—key skills needed by information warriors to conduct IO. The rationale in their approach is compelling. They argued that because information networks are weapons systems, and information is a center of gravity, the Air Force must develop world-class information warriors. The phrase they used was "to be one with the warfighters."[64] While a little melodramatic, it succinctly captures the essence of the challenge: To develop information operators with credentials readily acknowledged by other Air Force operators. Graduates of the C&I Weapons School would be awarded AFSC W33SX and assigned to unified commands and NAFs. There they would be the resident J6/A6 staff expert on friendly information systems employment, adversary information capabilities, and to develop exercises and plans to improve C&I integration in military operations.

Both of these approaches offer a good initial effort to develop information warriors, but neither one goes far enough. While the IOIC course is a step in the right direction, it's only a half step. As assessed by the Air Force's Intelligence staff, the course doesn't address the long-term educational needs to develop skilled information operators. And while the course provides IO training for many different AFSCs as a precursor to awarding the "U" Prefix for officer and enlisted IO warriors, the course only provides basic IW training and is "too narrow to capture the totality of IO tasks required by current doctrine."[65] In addition, for a variety of reasons, not the least of which is changing supply and demand, the Air Force has a poor track record of managing a limited number of people with special AFSC prefixes and matching them to jobs that require them.

The Weapon School's proposal is another step in the right direction but falls short because it proposes only to train 33S officers in IO and excludes all other AFSCs. While a well-intended effort to ensure 33S officers are prepared for future IO challenges, this proposal appears as an attempt by the 33S community to co-opt the AF's IO mission area for itself which probably guarantees that this approach will fail. The hope that 33S officers could go to a weapons school comprised of only 33S officers, study space and air operations, and gain credibility with other traditional Air Force operators is at best wishful thinking. A more comprehensive approach is needed. Instead of tinkering on the margins, the Air Force must commit to standing up an Information Operations career field that includes the participation of traditional operators, intelligence, and IT professionals. In this way, the Air Force can ensure the synergy needed to plan and execute effective IO.

An "information warrior" requires comprehensive education and skills. As Martin Libicki observed, "In the military, the challenge for the information warrior is not only to know the technical side of information systems but to understand the warfighter's needs: the commander's intent, doctrine and strategies. The amount of information necessary to be an information warrior is immense, and the time

required to master it will have to be at the expense of more general command instruction."[66] Martin Libicki's observation helps establish some important criteria for an Air Force IO career field.

It's time for revolutionary change. The legacy career fields that helped win the cold war, with cold war technologies, must give way to organizations and career fields that adapt to new operational realities and new technologies. We need to do away with the present day functional stovepipes that keep the Air Force from exploiting common skills across IO-related mission areas. And finally, we need to integrate IO into the Air Force's corporate operational structure. A separate IO career field will make effective IO possible and information superiority a reality. Just as important, it will help the Air Force retain its IT professionals. What this Air Force IO career field could look like and what benefits the Air Force could gain from this initiative are discussed next.

AN AIR FORCE IO CAREER FIELD—CHARACTERISTICS, STRUCTURE, BENEFITS

The times change and we change with them.

—From Owen's Epigrammata [1615]

Standing up a separate IO career field in the military services is not unprecedented. The Army has already blazed the trail by creating a separate IO functional area (FA 30) within its Information Operations Career Field. Officers assigned to FA 30 are tasked "to integrate all efforts to protect the Army's command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) with other IO capabilities; attack adversary C4ISR; and respond to potentially hostile C4ISR. FA 30 officers integrate the execution of offensive and defensive IO to gain information superiority in support of a warfighting commander's concept of operation. As such they are integral to every phase of Army and joint planning and operations."[67]

The Army's IO functional area links the following capabilities to achieve IO objectives: operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), physical destruction, civil affairs (CA) and public affairs (PA). "IO officers synchronize IO actions to help fulfill the commander's intent, provide critical information for decision-making and exploit information advantages. The IO functional area is employed to support commanders of the unified commands; the joint staff; DoD agencies; Department of the Army (DA) and its major commands; and Army warfighting organizations."[68] While beyond the scope of this paper, examining FA 30's unique features and career life cycle could help baseline the characteristics and structure of an Air Force IO career field.

Any new Air Force Information Operations career field must—at a minimum—satisfy the following criteria to improve service and joint IO planning and execution, gain corporate warfighter buy-in, and improve the job satisfaction of IT professionals:

- Develop world-class "information warriors"—operators educated, trained and skilled to plan and execute dominant IO for warfighters across the spectrum of military operations.
- Create synergy by exploiting skills across operations, intelligence, and IT career fields.
- Provide a self-sustaining career (O-1 to O-6) that enjoys equitable opportunities for success with other AF operations career fields: education, training, assignments and promotions.
- Leverage psychological motivators, like training, to improve job satisfaction and IT retention.

In addition, the following criteria are desirable:

- Use existing resources—budget and force strength.
- Improve AF return on investment (ROI) for IO education and training.
- Provide incentives for follow-on government service after military retirement to help the Federal sector protect the nation's critical infrastructures.

A notional officer IO career path that attempts to satisfy these essential and desirable criteria is described below. Underlying this model are two critical assumptions. 1) The education, training, and skills needed to conduct IO and win information superiority must be cultivated over the course of one's

career; and 2) Relevant intrinsic and non-intrinsic (psychological) incentives must be used to promote retention and to improve the Air Force's ROI. Achieving information superiority will require officer and enlisted IO warriors; however for simplicity, description of an enlisted IO career path is not provided. A construct similar to the notional IO officer career path described below is easily envisioned using relevant incentives, like 2- and 4-year college degrees at appropriate enlisted career decision points, and bonuses for attaining IO-required technical certifications. Appropriate active duty service commitments (ADSC) should also be accrued for AF-financed training.

A NOTIONAL AIR FORCE IO OFFICER CAREER PATH

- Future IO warriors will be assessed and initially train and serve in the following specialties: Intelligence (14N); Communications-Computer Systems (33S); and any of the following operational specialties: Reconnaissance, Surveillance, or Electronic Warfare Pilot (11R); Air Battle Management, (13B); Combat Control, (13D); Space and Missile Operations, (13S); and Command and Control, (86P). Public Affairs (35P) officers could also be considered.
- Between 6 and 7 years-of-service, high performing Captains, fully qualified in their entry specialty, are competitively selected to enter the IO career field. They then attend a basic, yet rigorous, IO course—12-months of training to equip the officer with foundational, cross-functional IO education and skills in operations, intelligence and information technology. Officers are selected based on the needs of the Air Force, performance, and perhaps by considering their previous education. If not previously attended, officers selected for the IO career field attend Squadron Officers School (SOS) prior to the Basic IO Course.
- Following graduation from the Basic IO Course, officers incur a 3-year ADSC. They are then employed in an appropriate "apprentice/journeyman" level IO job on a AF Major Command (MAJCOM) staff; Numbered Air Force (NAF) Information Warfare Flight (IWF); the Air Force Information Warfare Center (AFIWC); or defense agency, like the Defense Information Systems Agency (DISA). The objective during any initial assignment is to gain operational and tactical IO training and skills.
- Between 10 and 11 years-of-service, high performing IO officers, Major-Selects, are competitively selected to attend the Air Force Institute of Technology (AFIT) or a civilian university to earn a Masters Degree in an IO-related discipline. Prior to, or after earning their Masters degree, selected officers attend Intermediate Service School (ISS).
- Following graduation with their Masters Degree, IO officers incur a 3-6 year ADSC depending on the length of their program. (ADSC for ISS graduation is served concurrently). Graduates are then assigned to increasingly demanding "journeyman/supervisory" level jobs to support unified commands; the joint staff; DoD agencies; HQ USAF, AF MAJCOMs, NAFs and AF IO units worldwide. These officers are well qualified to staff a JFC's IO cell and would reduce the staffing now required by many functional areas.

- Between 14 and 17 years of service, high performing IO officers, now Majors/Lt Col-selects, must perform 1-year career broadening IO-related duty in the public or private sector. Completion of this 1-year duty will incur an additional 3-year ADSC.
- Between 17 and 20 plus years of service, high performing IO officers, now Lt Col/Col-selects will attend Senior Service School (SSS) and be assigned the most demanding IO jobs inside and outside DoD. These officers will command AF and Joint IO organizations and lead unified command and AF staffs. Due to their broad education, training, and experience, these officers are extremely well qualified to lead a joint IO cell to plan and execute a JFC's IO campaign or to lead AF-only IO operations.
- To incentivize 30 years of military service, well qualified IO professionals could be offered appropriate GS-13/14 or GS-15 civilian jobs in the Federal Government to help relieve the shortage of qualified people tasked to protect the nation's critical information infrastructures.

BENEFITS OF AN AIR FORCE IO CAREER FIELD

Creating an Air Force IO career field as described above would deliver many benefits to the Air Force, warfighting commanders and the Nation to include:

- Developing "world-class" IO warriors. Provides the means to accrue the "immense" education, training and skills essential to plan, coordinate and execute effective IO.
- Improving AF lethality. Integrates warfighting and IT specialties, creating synergy to execute IO and lead-turn the enemy's decision loop. Completes AF operations community; acknowledges information is a potential weapon and potential vulnerability. Provides better skill sets to master the battlespace.
- Clarifying what business IT professionals are in—information operators vice technology providers; military-essential information "warrior" versus "contractor provided "systems support." Clear operational career track answers the question: What military-essential business should "bluesuit" IT providers be in? Functions not essential to conducting IO become unambiguous candidates for CS&P. Leverages current 33S manpower; instead of trying to do "everything" permits focusing on the "right things." Could result in further 33S manpower "savings" while providing real incentives for 33S retention.
- Satisfying the Secretary of the Air Force's concern on officer overspecialization. An IO career field will broaden AF officers as they master various cross-functional disciplines in operations, intelligence, and information technology.
- Helping to neutralize the "Dilbert" factor. An operational IO career track would develop smart IO mentors: commanders, supervisors, and trainers through the grade of Colonel.
- Improving IT retention. Provides psychological satisfaction by offering military professionals training and an opportunity "to do IO"—warrior functions not available in the private sector.
- Providing the AF better return on IO training investments.

- Streamlining joint IO planning and operations. Instead of myriad people and the inefficient IO cell now required to develop an IO campaign, a cadre of IO warriors would create the catalyst for much simpler IO planning organizations at the joint and service levels. With expertise in most of the operational and technical areas required to plan, coordinate and execute successful IO, fewer people would be required to staff the warfighter's IO cell.
- Providing experts to more effectively develop good joint and service IO doctrine and execute it. Smart doctrine written by full-time practitioners and smart IO "trigger-pullers" will understand the strategic and operational implications of tactical information operations and be better equipped to explain the implications to civilian decision-makers.
- Keeping IO experts employed in the government. With appropriate incentives, retiring military IO professionals could help the Federal Government protect the nation's critical infrastructures. According to Mark Montgomery, the White House's Director of Critical Infrastructure Protection for the National Security Council, "The current practice of contracting out administration of government computer networks is not a good model for information security. We're trying to develop a system so you don't have to contract out for management and security administration of our information technology networks. It creates a more secure environment if we hire and train our own workers."[69]

CONCLUSION

In no other profession are the penalties for employing untrained personnel so appalling or so irrevocable as in the military.[70]

—General Douglas MacArthur,
US Army Chief of Staff, 1933

Achieving information superiority is a complex challenge demanding people with multi-faceted skills. To achieve it we must develop and retain "information warriors"—practitioners with special skills in the art of executing information operations. Information operations have been characterized as, "a future opportunity, competition, and vulnerability—all at once."[71] As the National Defense Panel observed, "We must never forget that our people in uniform have been the core of our strength in the past. They, more than any hardware system, form the real defense capability of today and tomorrow. Under no circumstances should we reduce the quality or training of our people. The technology revolution and advanced weapons we seek to embrace will be for naught if we take our military and civilian work force for granted."[72]

We must think beyond 2010 and build the capability to conduct skillful information operations in the future. Standing up an Air Force IO career field is essential to meet our future mission responsibilities and will help us take better care of Air Force people. We must prepare today for tomorrow's information fight. Developing "information warriors" is the way we'll win. Let's get on with it!

WORD COUNT = 8552.

ENDNOTES

[1] Department of the Air Force, 609th Information Warfare Squadron (IWS): A Brief History, Oct 1995 – Aug 1997, (Shaw Air Force Base: 609th IWS, September 1997), cover page.

[2] Joint Chiefs of Staff, Joint Vision 2010 (JV 2010), (Washington D.C.: Office of the Joint Chiefs of Staff, Summer 1996), 16.

[3] Ibid., 19.

[4] The Joint Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (JP3-13) (Washington D.C.: Office of the Joint Chiefs of Staff, 9 October 1998), III-1.

[5] Bill Gertz, "China Plots Winning Role in Cyberspace." November 17, 1999. Available from <http://ebird.dtic.mil/Nov 1999/e19991117plots.htm>; Internet; accessed 17 November 1999.

[6] Ibid.

[7] Bill Gertz, "Internet Warfare Concerns Admiral." November 18, 1999. Available from https://ca.dtic.mil/cgi-bin/ebird; Internet; accessed 18 November 1999.

[8] JV 2010, 10.

[9] Bill Gertz, "China Plots Winning Role in Cyberspace." November 17, 1999. Available from http://ebird.dtic.mil/Nov 1999/e19991117plots.htm; Internet; accessed 17 November 1999.

[10] Bill Gertz, "Computer hackers could disable military; System compromised in secret exercise," Washington Times, April 16, 1998, p. A1.

[11] William S. Cohen, Annual Report to the President and the Congress, (Washington D.C.: U.S. Government Printing Office, 1999), 18.

[12] Glenn D. Watt, "Self-Inflicted System Malfunctions Threaten Information Assurance," Signal, July 1999, 61.

[13] U.S. Department of Defense, Defense Science Board Task Force (DSBTF) on Information Warfare – Defense (IW-D), (Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996), 6-26.

[14] Ibid.

[15] Ibid., 6-27.

[16] Michelle L. Hankins, "Social, Criminal Protagonists Engage in New Information Age Battle Techniques," Signal, July 1999, 53.

[17] Ibid., 54.

[18] Department of the Air Force, Air Force Doctrine for Information Operations, Air Force Doctrine Document 2-5 (AFDD 2-5), (Washington D.C.: U.S. Department of the Air Force, 5 August 1998), 3.

[19] Sun Tzu, The Art of War, trans. by Samuel B. Griffith (Oxford: Oxford University Press 1963), 77.

[20] JP3-13, I-9.

[21] Ibid., I-11.

[22] Ibid., I-10.

[23] Ibid., inside front cover.

[24] John M. Shalikashvili, National Military Strategy of the United States of America, (Washington D.C.: Department of Defense, September 1997), 27.

[25] JP 3-13, I-10.

[26] Ibid., IV-3.

[27] David W. Lamm, Colonel, United States Army, interview by author, 11 February 2000, Carlisle, PA.

[28] JP 3-13, IV-2.

[29] AFDD 2-5, 7.

[30] Ibid., I-5.

[31] A.J. Bosker. February 2, 2000. "AF Holds Summit to Stem Tide in Retention." Available from http://www.af.mil/newspaper/v2_n4_s1.htm; Internet; accessed 7 February 2000.

[32] U.S. Department of Defense, First-Term Enlisted Attrition Report, (Washington, D.C.: U.S. Department of the Defense, 23 October, 1998), 25.

[33] Office of Economic and Manpower Analysis, Where Have All the Captains Gone? (West Point, N.Y.: United States Military Academy, August 1998), 5.

[34] George Woodward. April 7, 1999. "Give Current Initiatives a Chance, says PACAF Commander." Available from <http://www.af.mil/news/Apr1999/n19990407_990613.html>; Internet; accessed 7 February 2000.

[35] The Information Technology Association of America, "Help Wanted 1998: A Call for Collaborative Action for the New Millennium," March 1998, 6.

[36] Department of Commerce, "America's New Deficit: The Shortage of Information Technology Workers," Report of the Office of Technology Policy, undated, 3.

[37] Ibid.

[38] Avron Barr and Shirley Tessler. March 3, 1997. "The Software Shortage." Available from http://www-scip.stanford.edu/group/scip/avsgt/swlabor397.pdf; Internet; accessed 28 December 1999.

[39] Department of Commerce, "America's New Deficit: The Shortage of Information Technology Workers," Report of the Office of Technology Policy, undated, 17.

[40] Ibid.

[41] Ibid., 12.

[42] Office of the Secretary of Defense, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," August 27, 1999, A-1.

[43] General Montgomery Meigs <cg@cmdgrp.hqusareur.army.mil>, "Information Assurance," electronic mail message to General Eric Shinseki, 29 March 1999.

[44] Department of the Air Force, Posture Statement 1999, undated, 20.

[45] Lisa McCoy, "Building the Team....Communications and Information Professional Force Outlook," briefing slides with scripted commentary, Scott Air Force Base, Air Force Communications Agency, 30 November 1999.

[46] Ibid.

[47] Michael Brown, "Information Operations: IO Council of Colonels," briefing slides, HQ Department of the Army, Washington D.C., 2 November 1999.

[48] Ibid.

[49] Abraham H. Maslow, Motivation and Personality, (New York: Harper and Rowe, 1954), 19.

[50] Frederick Herzberg, Work and the Nature of Man, (New York: The World Publishing Co., 1966), 81.

[51] Michael Brown, "Recruiting and Retention," briefing slides, HQ Department of the Army, Washington D.C., 17 February 2000.

[52] Lisa McCoy, "Building the Team....Communications and Information Professional Force Outlook," briefing slides with scripted commentary, Scott Air Force Base, Air Force Communications Agency, 30 November 1999.

[53] Ibid.

[54] Ibid.

[55] CMS Greg Dahene, AFCA/XPFF, telephone interview by author, 15 October 1999.

[56] Lisa McCoy < lisa.mccoy@scott.af.mil>, "More Retention Info: General William Donahue Interview with Government Computer News, 26 July 1999," electronic mail message to Russ Miller <rusty1@pa.net>, 1 December 1999.

[57] A.J. Bosker. February 2, 2000. "AF Holds Summit to Stem Tide in Retention." Available from http://www.af.mil/newspaper/v2_n4_s1.htm; Internet; accessed 7 February 2000.

[58] Bob Brewin, "Civilian IT Pay Thwarts Army: Project Launched to Find Ways to Keep IT Personnel." October 18, 1999. Available from <http://ebird.dtic.mil/Oct 1999/e199910197plots.htm>; Internet; accessed 20 October 1999.

[59] Ibid.

[60] Lisa McCoy < lisa.mccoy@scott.af.mil>, "More Retention Info: General William Donahue Interview with Government Computer News, 26 July 1999," electronic mail message to Russ Miller <rusty1@pa.net>, 1 December 1999.

[61] JV 2010, 30.

[62] AFDD 2-5, 34.

[63] Lance Spencer and Mike Stinson, "Communications & Information Division USAF Weapons School," briefing slides, Nellis Air Force Base, USAF Weapons School, 17 June 1999.

[64] Ibid.

[65] Jackie Walsh, "Reorganizing for Information Operations: A Thinkpiece for IO 2010," briefing slides, Headquarters, Department of the Air Force, AF/XOIIIFM, 12 August 1998.

[66] Dr Martin C. Libicki and Commander James A. Hazlett, "Should there be an Information Corps?", Joint Forces Quarterly, Autumn 1993, 93.

[67] Department of the Army, "Functional Area 30 – Information Operations." Available from <http://www-cgsc.army.mil/dao/fa30/WhatisFA30.htm>; Internet; accessed 15 February 2000.

[68] Ibid.

[69] Elizabeth Shogren. November 23, 1999. "U.S. Tries To Plug Computer Worker Drain." Available from http://ebird.dtic.mil/nov1999/e19991123ustries.htm; Internet; accessed 1 December 1999.

[70] JP 3-13, VI-4.

[71] National Defense Panel, "Transforming Defense: National Security in the 21st Century," Report of the National Defense Panel, December 1997, 13.

[72] Ibid., iii.

BIBLIOGRAPHY

Barr, Avron and Tessler, Shirley. "The Software Shortage." March 3, 1997. Available from <http://www-scip.stanford.edu/group/scip/avsgt/swlabor397.pdf>. Internet. Accessed 28 December 1999.

Brown, Michael. "Recruiting and Retention." Briefing slides. Washington D.C.: Headquarters, Department of the Army, 17 February 2000.

Chairman of the Joint Chiefs of Staff. Joint Vision 2010. Washington D. C.: Office of the Joint Chiefs of Staff, Summer, 1996.

Clinton, William J. A National Security Strategy for a New Century. Washington D.C.: U.S. Government Printing Office, October 1998.

Cohen, William S. Annual Report to the President and the Congress. Washington D.C.: U.S. Government Printing Office, 1999.

Dahene, Greg, AFCA/XPFF. Telephone interview by author, 15 October 1999.

Gertz, Bill. "China Plots Winning Role in Cyberspace." November 17, 1999. Available from <http://ebird.dtic.mil/Nov 1999/e19991117plots.htm>. Internet. Accessed 17 November 1999.

Gertz, Bill. "Internet Warfare Concerns Admiral." November 18, 1999. Available from <https://ca.dtic.mil/cgi-bin/ebird>. Internet. Accessed 18 November 1999.

Hankins, Michelle L. "Social, Criminal Protagonists Engage in New Information Age Battle Techniques," Signal, July 1999, 53-54.

Herzberg, Frederick. Work and the Nature of Man. New York: The World Publishing Co., 1966.

Information Technology Association of America (ITAA). "Help Wanted 1998: A Call for Collaborative Action for the New Millennium," Arlington, VA, March 1998.

The Joint Staff. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington: The Joint Staff, 9 October 1998.

Libicki, Martin C. and Hazlett, James A. "Should there be an Information Corps?" Joint Forces Quarterly, Autumn 1993, 88-97.

Maslow, Abraham H. Motivation and Personality. New York: Harper and Rowe, 1954.

McCoy, Lisa. "Building the Team....Communications and Information Professional Force Outlook." Briefing slides with scripted commentary. Scott Air Force Base: Air Force Communications Agency, 30 November 1999.

McCoy, Lisa. < lisa.mccoy@scott.af.mil>. "More Retention Info: General William Donahue Interview with Government Computer News, 26 July 1999." Electronic mail message to Russ Miller <rusty1@pa.net>. 1 December 1999.

Meigs, Montgomery. <cg@cmdgrp.hqusareur.army.mil>. "Information Assurance." Electronic mail message to General Eric Shinseki. 29 March 1999.

Office of Economic and Manpower Analysis. Where Have All the Captains Gone? West Point, N.Y.: United States Military Academy, August 1998.

Office of the Secretary of Defense, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," August 27, 1999.

President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructure. Washington D.C.: The White House, October 1997.

Report of the National Defense Panel, "Transforming Defense: National Security in the 21st Century," December 1997.

Report of the Office of Technology Policy, "America's New Deficit: The Shortage of Information Technology Workers," Department of Commerce, undated.

Shalikashvili, John M. National Military Strategy of the United States of America. Washington D.C.: Department of Defense, September 1997.

Shogren, Elizabeth. "U.S. Tries To Plug Computer Worker Drain." November 23, 1999. Available from http://ebird.dtic.mil/nov1999/e19991123ustries.htm. Internet. Accessed 1 December 1999.

Spencer, Lance and Stinson, Mike. "Communications & Information Division USAF Weapons School." Briefing slides. Nellis Air Force Base: USAF Weapons School, 17 June 1999.

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

U.S. Department of the Air Force. 609th Information Warfare Squadron (IWS): A Brief History, Oct 1995 – Aug 1997. Shaw Air Force Base: 609th IWS, September 1997.

U.S. Department of the Air Force. Air Force Doctrine for Information Operations. Air Force Doctrine Document 2-5. Washington D.C.: Department of the Air Force, 5 August 1998.

U.S. Department of the Air Force. Posture Statement 1999. Washington D.C.: Department of the Air Force, undated.

U.S. Department of the Army. "Functional Area 30 – Information Operations." Available from <// http://www-cgsc.army.mil/dao/fa30/>. Internet. Accessed 5 February 2000.

U.S. Department of the Army. "OPMS XXI Briefing." 18 May 1999. Available from <http://www.army.mil/opms/>. Internet. Accessed 5 February 2000.

U.S. Department of Defense. Acquisition Career Development Program. Department of Defense Directive 5000.52.M. Washington D.C.: Office of the Under Secretary for Defense for Acquisition and Technology, November 1996.

U.S. Department of Defense. Defense Science Board Task Force on Information Warfare - Defense. Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996.

U.S. Department of Defense. First-Term Enlisted Attrition Report. Washington, D.C.: U.S. Department of the Defense, 23 Oct 1998.

U.S. Department of Defense. Information Operations. DoD Directive S-3600.1. Washington D.C.: U.S. Department of Defense, 9 December 1996.

Walsh, Jackie. "Reorganizing for Information Operations: A Thinkpiece for IO 2010." Briefing slides. Washington D.C.: Headquarters, Department of the Air Force, AF/XOIIIFM, 12 August 1998.

Watt, Glenn D. "Self-Inflicted System Malfunctions Threaten Information Assurance," Signal, July 1999.