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.

EDUCATING JUNIOR MILITARY OFFICERS FOR THE INFORMATION AGE

BY

COLONEL ANDRE H. SAYLES
United States Army

19980605 083

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

USAWC CLASS OF 1998

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

DTIC QUALITY INSPECTED 4

USAWC STRATEGY RESEARCH PROJECT

Educating Junior Military Officers for the Information Age

by

COL Andre H. Sayles

Dr. Douglas V. Johnson II
Project Advisor

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.

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

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

ABSTRACT

AUTHOR: Andre H. Sayles (COL), USA

TITLE: Educating Junior Military Officers for the Information Age

FORMAT: Strategy Research Project

DATE: 1 April 1998 PAGES: 43 CLASSIFICATION: Unclassified

As pointed out in *Joint Vision 2010*, improvements in information and systems integration technologies will have a significant impact on future military operations. The phrase ***dominant battlefield awareness*** is used to describe an environment in which the commander will be able to monitor friendly and enemy operations in real time. Improved situational awareness is expected to be a product of the Information Revolution in which telecommunications, sensors, all sources of intelligence, and global positioning are integrated into a single system for the individual warrior. Decentralized operations will require leaders at the lowest level to understand information age technologies. Current senior military officers began active service before the personal computer became popular in the early 1980s. Military leaders entering the service in the year 2000 will be key staff officers in 2010 and the senior commanders in 2025. This report addresses the extent to which military leaders will need to be technologically literate in the information age and how we can get to where we need to be.

TABLE OF CONTENTS

ABSTRACT iii

LIST OF ILLUSTRATIONS vii

LIST OF TABLES ix

INTRODUCTION 1

INFORMATION OPERATIONS 3

INFORMATION AGE TECHNOLOGIES 6

FUTURE MILITARY SCENARIO 7

  CURRENTS OF CHANGE 8

  LAND WARRIOR FUTURES 9

  LAND WARRIOR SUPPORTING FORCES 9

  LAND WARRIOR TECHNOLOGY 10

SCENARIO INTERPRETATION 11

FUTURE LEADERSHIP CHALLENGES 13

OFFICER EDUCATION 16

WORK IN PROGRESS 24

CONCLUSION 26

ENDNOTES 29

BIBLIOGRAPHY 33

LIST OF ILLUSTRATIONS

Figure 1. Information Operations Relationships Across Time 4

Figure 2. Information Warfare Systems Engineering at NPS 25

LIST OF TABLES

Table 1. Education Requirements for Military Officers 17

Table 2. Education Opportunities for New Officers 22

INTRODUCTION

> Future military leaders need to learn about cutting-edge technology that may change how wars are fought, but they also need a historical underpinning to their professional education.
>
> — Rep. Ike Skelton[1]

As the Armed Forces transition to the 21st century, senior leaders will face the challenges of the information age. At an unprecedented pace, new technologies are changing the way the services plan for future military operations. During the first two decades of the next century, nearly every service member will feel the impact of the Information Revolution. A paradigm shift in the professional military education (PME) of junior officers is on the horizon. At the same time, this new approach to education must continue to provide for the historical underpinnings in the current education system.

In May 1996, the chairman of the Joint Chiefs of Staff published *Joint Vision 2010* as "the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."[2] This framework for joint operations in 2010 lays the foundation for visionary programs in the individual services.

The Army outlook for the first 25 years of the next century is captured by the continuum of *Force XXI*, *Army Vision 2010*, and

Army After Next.[3] Transitions for the Navy and Marine Corps will be guided by the strategic concept of *Forward ... From the Sea*.[4] The Air Force strategic vision is captured by *Global Engagement: A Vision for the 21st Century* and *Air Force 2025*.[5]

Joint operations are common threads that run throughout the collective vision of the chairman of the Joint Chiefs of Staff and the service chiefs. As a primary driving force behind future joint, combined, and ultimately integrated operations, the Information Revolution will lead to new education requirements for junior leaders. Soldiers , sailors, airmen, and marines will continue to win wars as they have done in the past. New technologies will not displace the human dimension. However, leaders will have to understand the tools of the trade in the future as they have in past wars. These new information age tools have already begun a historic revolution in military affairs (RMA).[6]

This study addresses some of the issues related junior military officer education in the information age. After a discussion of information operations (IO), a future scenario provides a basis for proposed junior officer education. This report suggests that education of military leaders be factored into ongoing force planning. The services should not assume that education requirements for the information age will be a natural product of the times. Unless direct action becomes a priority, the human factor may slow progress towards the 2010 force.

INFORMATION OPERATIONS

> All planning, particularly strategic planning, must pay attention to the character of contemporary warfare.
>
> — Carl von Clausewitz[7]

In 1996, Winn Schwartau defined information warfare (IW) as "those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary."[8] He developed this definition by combining elements of three existing taxonomies associated with the Department of Defense (DOD), national security, and economic infrastructure. Although the DOD focus was on actual conflict, the more broader definition offered by Schwartau extended to peacetime activities that ranged from recreational hacking to computer terrorism.

In FM 100-6, published in August 1996, the Army used information operations to describe the full range of information issues from peace through global war.[9] Information operations became the Army's implementation of the DOD version of information warfare, but in a much broader sense.

Although information warfare was becoming a universal term by the mid-1990s, a resistance to the use of "warfare" in the private sector ultimately led to a preference for information assurance (IA). This term described the full range of non-military activities related to what had previously been described as information warfare. The President's Commission on Critical

Infrastructure Protection described information assurance as:

> Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage. For instance, incident mitigation, incident response, and service restoration.[10]

Assurance includes protection of information systems, detection of intrusions, and restoration of operations after an attack. In 1998, the new Joint Publication 3-13 brought closure to the concept of military information operations from a Joint Staff perspective.[11] As shown in Figure 1, Joint Pub 3-13

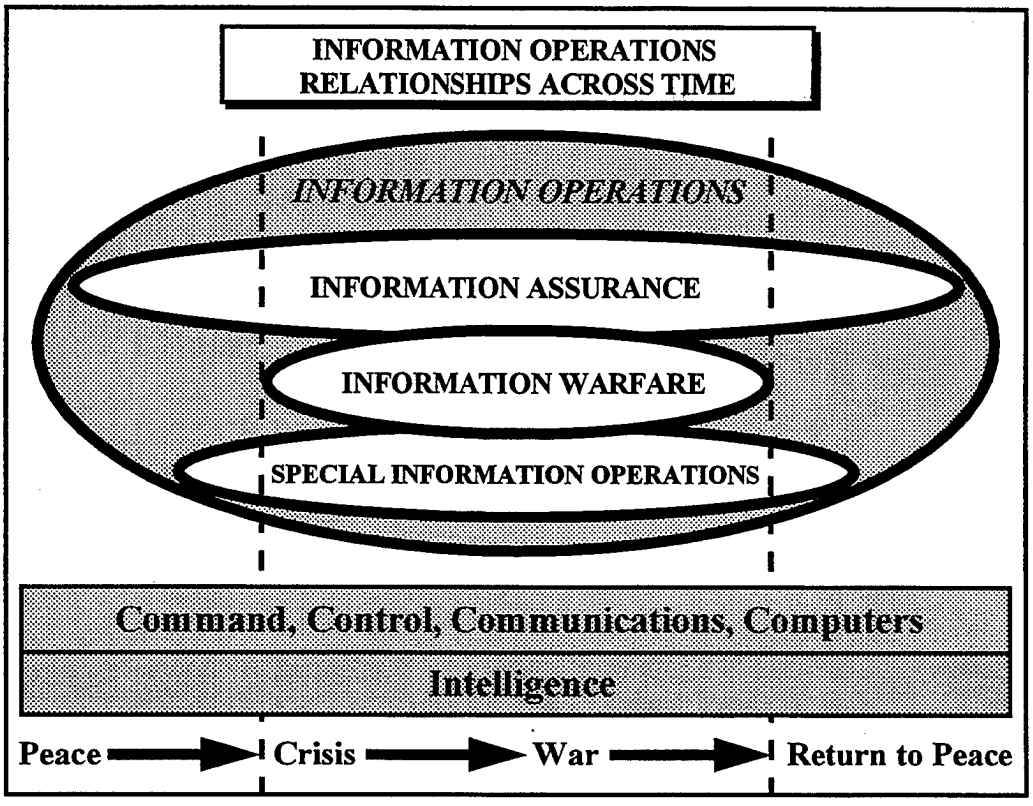

Figure 1. Information Operations Relationships Across Time

describes relationships between information operations, information warfare, and information assurance in peace and war.

Information operations are supported by command, control, communications, computers, and intelligence (C4I) across the full spectrum of military activities. Such operations include "actions taken to affect adversary information and information systems, while defending one's own information and information systems."[12] Information warfare is a subset of information operations during time of crisis or war. Like information operations, information assurance is a full-time activity. In Joint Pub 3-13, information assurance is defined as "IO that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation."[13] In DOD, as well as the private sector, information assurance implies protection of systems, detection of infringement, and recovery or reaction.

Defensive and offensive IO are relevant across the peace and war spectrum. Defensive IO is particularly important in protecting information systems on a daily basis. Information assurance is one of the many defensive measures available. As attacks on information systems continue to grow, offensive information operations will likely be used as defensive measures as well. Currently, the number of attacks on military information systems may be as high as 500,000 annually.[14] Many of these attacks are not detected by current defensive measures.

INFORMATION AGE TECHNOLOGIES

> The world has changed and there is great risk in standing still.
>
> — GEN Gordon R. Sullivan[15]

Information operations are a conduit for integration of information age technologies into future battlespace. The projections in *Joint Vision 2010* include global communications and intelligence networks, precision weapons, digitized platforms, direct links between sensors and shooters, advanced soldier systems, full enemy and friendly identification, and situational awareness.

Many of the rapidly advancing technologies are driven by new innovations in semiconductors, electronics, and optics. In 1965, Gordon Moore predicted that the number of transistors on an integrated circuit would double every year. In 1975, he revised his prediction to what is now called Moore's Law or the number of transistors will double every 18 months. Remarkably, his prediction has remained accurate for the past 20 years, except for very recent advances that are about one year early.[16]

Success in the semiconductor industry has underpinned advancement for many other technologies. Specifically, miniaturization of high speed processors has opened doors for computers, communication systems, sensors, displays, and numerous other capabilities that have both commercial and military applications. Coupled with advanced materials, signal

processing, and developments in software engineering, microelectronics has led to dramatic improvements in command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). Technology is affecting force structure, military operations, and the way the services manage information on a daily basis.

FUTURE MILITARY SCENARIO

> Generally, operations of war require one thousand fast four-horse chariots, one thousand four-horse wagons covered in leather, and one hundred thousand mailed troops.
>
> — Sun Tzu[17]

A significant number of futurists have offered scenarios describing the evolution of economic, political, social, and military conditions over the next 30 years. Likewise, each of the services has published a vision for the period from the present to 2025. Due to the conjectural nature of scenarios, an exhaustive review of military futures would offer no more certainty than a single brief scenario. Thus, a concise futurist statement is adequate to stimulate thoughts about junior officer education requirements in the information age. The following paragraphs offer a short future scenario based on the notion that the advanced land warrior will be the primary focus.

CURRENTS OF CHANGE

Steven Metz describes the most important overarching currents of change as interconnectedness, compression of time, and demassification.[18] At the strategic level, these three broad categories are applicable to many published military futures. Interconnectedness is already underway at all levels within the Armed Forces, including individual, organizational, service and interservice systems. The increased focus on information operations supported by C4ISR is but one indication that interconnectedness is a way of the future.

In both peace and war, the compression of time is becoming reality through a variety of communications and information systems. Data can be sent or retrieved in near real time from virtually any location on earth. Future transportation systems will likely compress both time and space as travel times are reduced or the need to travel long distances to accomplish the mission will no longer be necessary.

The application of demassification to military organizations will lead to smaller units across the services. The smaller units will be able to conduct an operation anywhere in the world while moving quickly and maintaining global communications. The full range of information operations resources will be at their disposal.

LAND WARRIOR FUTURES

Over the next 30 years, the land warrior will develop into an individual fighting machine. Outfitted in climate-controlled individual armor, the land warrior will be protected by an integrated defense against chemical agents, small arms fires, and adverse environmental conditions. Global communications via satellite will complement regional communications via wireless or cellular systems enhanced by unmanned aerial vehicles. Along with these communications assets, advanced global positioning concepts will be integrated into a specially designed helmet.

At the touch of a button or perhaps in response to an inconspicuous mental or physical gesture, the head-worn display will provide the positions of enemy and friendly forces, targeting information, mission status, and environmental conditions. The individual weapon will be able to identify and target the enemy while offering a range of responses from stun to kill. The land warrior will have no concerns about temporary environmental conditions such as day and night. Likewise, the ability to be extracted or re-supplied at just the right time is taken for granted.

LAND WARRIOR SUPPORTING FORCES

The remainder of the military force structure will be designed to support the individual land warrior as well as operate independently. A wide range of small units can be

combined at practically any level or size in order to provide the necessary firepower and logistical support. Heavier weapons can be made available in case of a rare conflict which may be thought of as conventional. Supporting aviation platforms range from close support to strategic. Space and naval assets are available to the land warrior upon request. When the mission dictates a larger force, land, air, and sea elements will be integrated into a single unit that communicates and operates much like the smaller land warrior component.

LAND WARRIOR TECHNOLOGY

The land warrior is a creation of the Information Revolution. From a technology point of view, only the land warrior assets matter in the transition to the future. Capabilities that have been miniaturized and powered for the land warrior in 2030 or the robot replacement in 2050 can easily be duplicated on larger platforms. Global communications, situational awareness, precision weapons, and climate-control are easily accomplished on vehicles, ships, and aviation assets where power, size, and weight restrictions are of less importance.

In some cases, existing larger platform technology will be miniaturized for land warrior use. In other cases, technology developed for the land warrior will be magnified for space, air, naval, and vehicular applications. The greatest challenge will

be developing resources for the land warrior. Integrating those capabilities into the other forces will be a secondary task.

Cyber tools will underpin nearly every land warrior asset. Addition of the land warrior support forces will generate an integrated battlespace that provides real-time C4ISR, logistics, and medical support. The battlespace will be supported by a national cyber infrastructure that is linked to an international infrastructure and a space infrastructure. Within this framework, wars will be fought -- sometimes from space, sometimes silently through the global cyber infrastructure, sometimes by the warrior support forces, and sometimes by the warrior on the ground.

SCENARIO INTERPRETATION

> Technology, one of the principal driving forces of the future, is transforming our lives and shaping our future at rates unprecedented in history, with profound implications that we can't even begin to understand.
>
> — John L. Petersen[19]

The scenario in the previous section is just one of the many ways of looking at the future. The complete credibility of such a projection into the future is not essential to an argument for or against a paradigm shift in junior officer education. In fact, when funding constraints are considered, the probability of the full set of advanced land warrior and support forces appearing in 2025 is relatively low. The most likely scenario is

one that projects a mixture of forces at various stages of modernization.

By 2025, the Armed Forces may have a percentage of advanced forces with a correspondingly advanced support structure. The remainder of the force may be grouped into two or three categories according to the level modernization. The extension of modernization to reserve forces is yet another consideration. Some of the more expensive platforms may essentially still exist as they do today, except for selected sub-system improvements.

The argument for a new look at junior officer education can be supported by any segment of the scenario, including projections for the next few years. The Information Revolution has already created a need for change, with a key step being the acknowledgment by DOD that information operations must be brought to the forefront. The implied education needs of the land warrior are already clear.

As outlined in *Joint Vision 2010*, "we must have information superiority: the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying and adversary's ability to do the same."[20] In time of conflict, offensive information warfare will reduce or eliminate enemy capabilities, while defensive information warfare will protect military operations as well as the supporting infrastructures.

Challenges associated with information assurance must be addressed on a full-time basis. Protection of national and space

infrastructures is vital to the safety and economic prosperity of America. These infrastructures invite attack at any time. Most attacks are recreational in nature. In time of conflict, it is likely that the infrastructures will invite more serious attacks as the adversary attempts to use space and cyberspace to further war aims.

For the land warrior, information superiority is the key to success, whether in the year 2000 or the year 2025. In an adverse environment, the land warrior must understand the technology that provides the tactical and operational advantage. This understanding must include how to use the technology effectively, how to make it work under adverse conditions, how to recognize when it is not functioning properly, and how to operate when the technology fails.

FUTURE LEADERSHIP CHALLENGES

> In no other profession are the penalties for employing untrained personnel so appalling or so irrevocable as in the military.
>
> — GEN Douglas MacArthur[21]

The impact of the Information Revolution on the Armed Forces has often been compared to the development of motorized armored vehicles and the effective use of technology in the Blitzkrieg of World War II. A parallel can be drawn between information age technologies and the internal combustion engine. Similarly,

Blitzkrieg can be likened to information operations and other methods of employing information age capabilities.

Perhaps a better analogy for pending revolutionary trends in military affairs is the impact of rifled and repeating weapons in the nineteenth century. The killing zone increased from approximately 150 meters to a thousand meters or more by the end of the American Civil War.[22] Many military leaders did not accept the larger killing zone brought on by technology and continued charge across open spaces while facing a rainstorm of bullets. Those who failed to respond to new weapons caused the loss many lives from Pickett's Charge at Gettysburg to the slaughters of World War I.

Like rifled and repeating weapons, information technologies will directly affect every person in uniform. At some point, C4ISR tools will be at the finger tips of every service member, including the land warrior. Those who fail to respond to the Information Revolution will join General Pickett at Gettysburg or the Allied Forces at the beginning of World War II. The services must face the need to bring warfighters into the information age. The most imminent challenge is the necessary paradigm shift in education of the officer corps. This change will be an even greater task for the services that have not emphasized technical degrees in the past.

The 1997 Army After Next Wargame demonstrated that tactical success depended to a great extent on the ability to execute

decentralized operations.[23] Junior leaders will have to be prepared to accomplish the mission without the luxury of calling upon support elements or contractors when equipment fails to operate properly. They must understand the underlying principles in order to use information age technologies to maximum effectiveness under a variety of conditions.

In the next century, information knowledgeable leaders at the small unit level will be expected to use the same communications and intelligence resources that digital technology will make available to higher commands. Education requirements will go well beyond the understanding of information technologies. At a higher level of complexity, integration of systems or "systems of systems" will require a general understanding of science and engineering along with a certain level of comfort with technical equipment. Training will not be able to accommodate the pace of change and the breadth of technological advances. The only solution will be through technical education for the officer corps.[24] This process must start with the undergraduate education of junior officers and continue through military education.

While education must focus on science, engineering, and the requisite historical perspective, both training and education should also address the need for leaders to make the correct decisions in a timespan decreased by the fast pace of future operations. Leaders must be decisive under conditions of too

much information, just enough information, and too little information. Quick and decisive development of innovative solutions to a wide-range of multi-dimensional problems will be a standard for good leadership. The information age will bring an overwhelming amount of information, but when systems have temporary failures the flood of information may become a drought.

OFFICER EDUCATION

> Wars may be fought with weapons, but they are won by men.
>
> — GEN George S. Patton, Jr.

The Armed Forces need "leaders who have a deep understanding of warfare in the context of the information age."[25] Such information knowledgeable leaders must have had the opportunity to internalize the significant capabilities and vulnerabilities associated with the current and future role of information (from both the technological and human perspectives).[26]

Although a variety of technologies will have an impact on future warfare, this study focuses on the information age. The Information Revolution is clearly the engine that is driving the revolution in military affairs and the need for a paradigm shift in junior officer education. When the services have an adequate number of information knowledgeable leaders, a likely by-product will be that the overall shortfall in science and engineering

education will become manageable. The result will be an environment in which technology is readily accepted.

The new approach to junior officer education must specifically address the four-year undergraduate program and the first six months of service after commissioning. The topics listed in Table 1 are suggested for three categories of military officer education by the end of the first year of service. Many of the topics can be covered in undergraduate programs if appropriate requirements are placed on commissioning sources.

	Depth of Knowledge		
TOPIC	TIER 1	TIER 2	TIER 3
Computers and Information Technology	B	I	A
Software Applications	B	I	I
Programming Languages	F	B	A
Software Development	N	F	I
Networks and Telecommunications	F	I	A
Information System Intruder Tactics	F	B	A
Information Security	F	I	A
Computer System and Network Security	F	B	A
Information Assurance	N	F	I
Human-Computer Interaction	F	B	B
Satellite Communications Systems	F	I	I
Global Positioning Systems (GPS)	F	B	B
Wireless Communications	F	B	I
Communications Fundamentals	B	I	I
Electrical Engineering Fundamentals	F	B	B
Electronic Vulnerabilities	F	B	I
Strategic and Operational Intelligence	B	A	A
Information Operations Principles	B	I	I

Levels: N-None F-Familiarization B-Basic I-Intermediate A-Advanced

Table 1. Education Requirements for Military Officers

The remaining topics can be provided through joint or service distance learning programs and military branch or specialty schools upon entry on active or reserve duty.

The depth of knowledge categories are represented by three tiers within the information operations knowledge domain. Tier 1 represents the minimum requirements for all junior officers. At this level of knowledge, all officers will have the tools to operate effectively and train subordinates in the information age or the land warrior scenario. Tier 2 represents the knowledge requirements for officers in branches or specialties that include operational level responsibilities in communications, intelligence or information. Finally, tier 3 is the depth of knowledge required of officers who have strategic level responsibilities or work as a scientist, engineer, or system administrator. Tier 3 officers are expected to have an undergraduate or graduate degree in science or engineering.

The topics in Table 1 do not imply separate academic courses. Single undergraduate courses that cover several of the topics already exist. An explanation of each topic follows:

Computers and Information Technology: This is a typical introductory or CS1 level computer course that provides the basics of computer operation, types of computers, and computer hardware. Completion of the course should enable the officer to be comfortable working with computers and displays at the required level.

Software Applications: Often included in introductory courses, software applications provide additional experience with computers and the opportunity to learn fundamentals that apply to commercial and military software.

Programming Languages: Languages provide an understanding of how software interfaces with hardware in computer systems, microprocessor-based systems, and military applications.

Software Development: At Tiers 2 and 3, military officers may be required to develop software, troubleshoot systems, or supervise contractors or military subordinates who perform those functions. Software is critical to system integration.

Networks and Telecommunications: Connectivity and communications between systems will be a primary component of future information warfare. Officers should have a minimum understanding of strengths and weaknesses in this area.

Information System Intruder Tactics: A first step in defense against attacks on information systems is the recognition of adversary techniques and capabilities. An understanding of the hacker will also lead to higher sensitivity on the part of the user and better identification of intrusions.

Information Security: The junior leadership in the military services will be expected to ensure proper security measures are in place for electronic information. Decentralization will place this responsibility at the lowest levels.

Computer System and Network Security: This topic includes computer system and communications security. The information warrior needs to understand security mechanisms and the associated vulnerabilities and reliability.

Information Assurance: Information assurance is a more advanced topic that focuses on maintaining robust systems that will resist attack, detect intrusions, and continue to operate while under attack. The technology for assured performance will evolve as infrastructure protection becomes a higher priority.

Human-Computer Interaction: Although not well defined, this topic will take on more importance as warfighters learn how to sort out information from the global communications and intelligence network. Subjects of interest include cognitive psychology and human decisionmaking.

Satellite Communications, Global Positioning Systems, and Wireless Communications: Leaders must be familiar with these three subjects since they will underpin future information operations. System level familiarization should be combined with a clear understanding of vulnerabilities to the environment as well as the adversary.

Communications Fundamentals: Every leader in the information age will be a communications officer. Computers will become so common that the user will be a system administrator to a large extent. The organizational system administrators will have to concentrate on architecture and security and will no longer be

able to make desk calls. The individual land warrior will have to know the communications business in this same manner.

Electrical Engineering Fundamentals: The information age would not exist without electronics. Future hardware will be based on advanced applications of electrical engineering principles. A low-level understanding of electronics will raise the confidence of users of numerous systems.

Electronic Vulnerabilities: Electronic vulnerability is a sub-topic of several of the other subjects, but is listed separately because this will be the adversary's primary counter measure in a theater of operations. Satellites, GPS, and many other information age technologies will be susceptible to degradation by electronic counter measures.

Strategic and Operational Intelligence: Situational awareness will be critical to warfighting in the next century. Intelligence information will be important at all levels from the individual land warrior to the carrier battle group. The information knowledgeable leader will need to know the sources of intelligence, the integration schemes, and how to interpret information in real time.

Information Operations Principles: Information operations are not confined to DOD. Many of the issues and concerns are common to the private sector. The importance of IO dictates that the principles be taught from an education perspective in an academic environment as well as in a training environment.

The implementation of an education program for military leaders will demand further study. The arguments presented here are by no means exhaustive. The topics in Table 1 are repeated in Table 2, along with suggestions as to how the required education can be provided. The services may have to place more requirements on commissioning sources and restrict the number of new officers who do not have a degree in mathematics, science, or

TOPIC	Undergraduate Course	Distance Learning	Military Course
Computers and Information Technology	X		
Software Applications	X		
Programming Languages	X		
Software Development	X		
Networks and Telecommunications	X		X
Information System Intruder Tactics	X	X	X
Information Security	X		X
Computer System and Network Security	X		X
Information Assurance			X
Human-Computer Interaction	X		X
Satellite Communications Systems		X	X
Global Positioning Systems		X	X
Wireless Communications		X	X
Communications Fundamentals	X	X	X
Electrical Engineering Fundamentals	X	X	
Electronic Vulnerabilities		X	X
Strategic and Operational Intelligence		X	X
Information Operations Principles		X	X

Table 2. Education Opportunities for New Officers

engineering. Joint distance learning programs may be more efficient than programs generated by individual services. It is important to again note that the service can no longer accomplish competency objectives through training. Education will have to play a much greater role in providing backgrounds that offer versatility and an acceptable level of comfort across a wide range of technologies.

The "military course" category in the right column of Table 2 would likely be the basic course or specialty training that a new officer receives upon entrance on active or reserve duty. Because of the importance of information age technologies, it is conceivable that most basic-level courses for new officers will have an information operations component in the next century.

The table may appear to suggest a large number of sub-courses under military education; however, the suggested tier 1 familiarization will often be a by-product of an undergraduate program. For example, satellite communications, GPS, and wireless technology may turn out to be survey topics in a communications course. On the other hand, the depth required at tier 3 may dictate a special sub-course if the undergraduate program for a particular officer did not meet expectations.

Information operations need not challenge warfighters in the next century as Blitzkrieg did in World War II. The American Army responded to German armored divisions by identifying officers who had the education to become leaders in newly formed

armored units. Since these units had not existed before, the Army could not look to training for the solution. Instead, versatile officers were identified from their education background. Education offers the same versatility necessary in the information age. As suggested by Alvin and Heidi Toffler, the new military must place massive emphasis on training and education at every level.[27]

WORK IN PROGRESS

> New technologies and processes can frighten those who are comfortable with the routines established to accommodate the old technologies. Furthermore, vested interests within the organization and within its bureaucracy—usually for what to them are good and logical reasons—will resist ideas that threaten status quo.
>
> —GEN Gordon R. Sullivan and LTC Anthony M. Coroalles[28]

The Department of Defense is leading the way in bringing information operations into focus. The establishment of a new deputy assistant secretary position for information operations and the pending publication of Joint Pub 3-13 will lead to increased emphasis on policy and doctrine. New technologies will eventually stimulate new ideas on force structure and staff organizations. As history as proven, the human dimension is of critical importance and must not be left out.

In August 1996, the Army published FM 100-6. Although the release of Joint Pub 3-13 will require significant revisions, FM

100-6 was a good start. In 1995, the Naval Postgraduate School (NPS) introduced an Information Warfare degree within the Systems Engineering Program. With the help of the Deputy Director of Operations, J39 (Information Operations), on the Joint Staff, the Navy has made a strong statement that officer education requirements have changed. An outline of the curriculum is available on the NPS web site and summarized in Figure 2 below. In addition to programs at the Naval Postgraduate School, the Navy established the Navy Information Warfare Activity in 1994 and the Fleet Information Warfare Center in 1995. Navy doctrinal

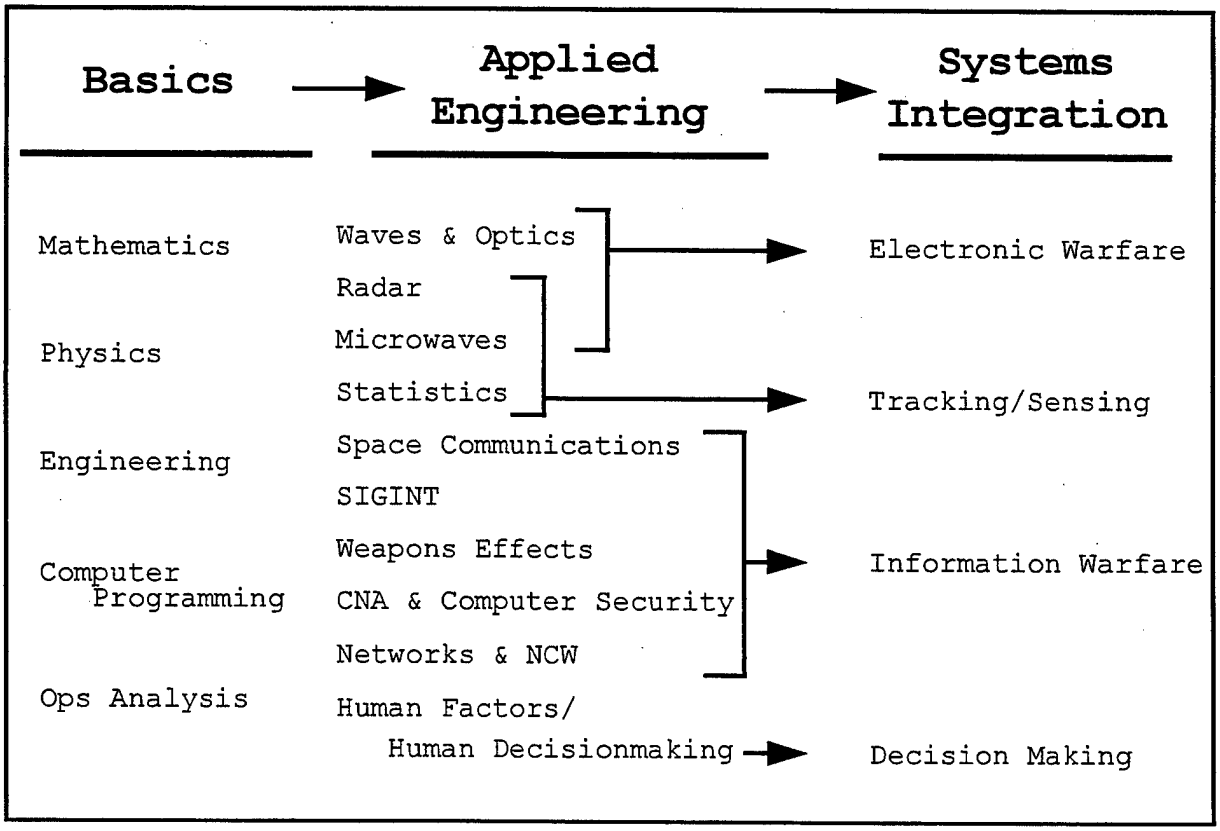

Figure 2. Information Warfare Systems Engineering at NPS[29]

publications will be published shortly after release of Joint Pub 3-13.

The Air Force established the Air Force Information Warfare Center in 1993 and created the 609th Information Warfare Squadron in 1996. In March 1997, the Air Force activated the Information Warfare Battlelab at the Air Intelligence Agency, Kelly Air Force Base, Texas. The Army's Land Information Warfare Activity has taken on a leadership role in establishing security measures for the information infrastructure and responding to attacks.

These are but a few examples of the DOD investments in the information age. The new Defense Information Assurance Program will add to ongoing efforts to secure the defense and national information infrastructure. Other initiatives will continue to address the full spectrum of offensive and defensive operations.

CONCLUSION

> We face no imminent threat, but we do have an enemy—the enemy of our time is inaction.
>
> — President William J. Clinton[30]

The next 10 years will be a critical time for American Armed Forces. Each of the services has charted out a path to 2010 and beyond with technology being a primary driving force. The manner in which leaders will be educated for *Joint Vision 2010* has not been adequately spelled out. Since the services will not reap

the benefits of any new education policy until approximately five years after the effective date, immediate action is necessary.

Over the next nine years the New York Times estimates that one million new computer science jobs will be created in the United States. Up to 400,000 jobs may be vacant in 1998.[31] With colleges and universities graduating less than 40,000 candidates for those jobs on an annual basis, the salaries offered to experienced programmers are sometimes exceeding six figures.

After the end of the Cold War, the services lost a large number of officers with technical degrees. Promotion policies have also been costly as officers who took time out to get advanced technical degrees were no longer competitive in the services. Although some of those officers have reserve commitments, many will not play a role in the next military force.

The demands of the Information Revolution are leading the services—some more than others—to the idea of contracting technical jobs to private companies. This idea has at least three major drawbacks. Due to competition in the private sector, the cost of private contracting and consulting to the military will be much more than the cost of requiring officers to come into the service with a technical degree. The services simply will not be able to afford the contracts. Today, a contract for a single civilian programmer costs up to $150,000 per year.

The second shortcoming is that contractors will not be willing to follow the warfighters into battle when so many jobs are available across the private sector. The third consideration is the evidence presented in this report that the need for technical competency will extend down to the small unit leader. We simply will not be able to hire a contractor to be the land warrior or land warrior leader.

In conclusion, the Armed Forces must strongly consider initiating programs that will develop information knowledgeable leaders. These programs must provide many more technically qualified officers than actually needed because of the expected losses to the private sector after service obligations are fulfilled. Junior officers will have to be educated through a combination of undergraduate course requirements, distance learning, and military schooling.

(6,000 Words)

ENDNOTES

[1] Rick Maze, "Officer Schooling Concerns Buyer, Skelton," Army Times, 16 February 1998, 6.

[2] John M. Shalikashvili, Joint Vision 2010 (Washington, D.C.: Chairman of the Joint Chiefs of Staff, 1996), 1.

[3] Dennis J. Reimer, Army Vision 2010 (Washington, D.C.: Department of the Army, 1996), 2.

[4] Department of Defense, Defense 97 (Alexandria, VA: American Forces Information Service, no. 6, 1997), 19.

[5] Ibid., 19.

[6] Steven Metz and James Kievit, Strategy and the Revolution in Military Affairs: From Theory to Policy (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 27 June 1995), v.

[7] Carl von Clausewitz, On War, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 220.

[8] Winn Schwartau, Information Warfare (New York: Thunder's Mouth Press, 2nd ed., 1996), 12.

[9] Department of the Army, Information Operations, FM 100-6 (Washington, D.C.: U.S. Department of the Army, 27 August 1996), 2-2.

[10] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure (Washington, D.C.: President's Commission on Critical Infrastructure Protection, 13 October 1997), B-2.

[11] Department of Defense Joint Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Draft) (Washington, D.C.: U.S. Department of Defense, 28 January 1998), I-4.

[12] Ibid., I-19.

[13] Ibid., I-18.

[14] John T. Correll, "War in Cyberspace," Air Force Magazine, January 1998, 34.

[15] Gordon R. Sullivan and Anthony Coroalles, The Army in the Information Age (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 31 March 1995), 21.

[16] Linda Geppert and William Sweet, "Technology 1998," Spectrum, January 1998, 20.

[17] Sun Tzu, The Art of War, trans. Samuel B. Griffith (Oxford, England: Oxford University Press, 1963), 72.

[18] Steven Metz, Strategic Horizons: The Military Implications of Alternative Futures (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 7 March 1997), 2-3.

[19] John L. Petersen, The Road to 2015 (Corte Madera, CA: Waite Group Press, 1994), 27.

[20] Shalikashvili, 16.

[21] Department of Defense Joint Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Draft) (Washington, D.C.: U.S. Department of Defense, 2 July 1997), VI-9.

[22] Department of the Army, The Annual Report on The Army After Next Project (Washington, D.C.: U.S. Department of the Army, July 1997), A-1.

[23] Ibid., 21.

[24] U.S. Air Force Scientific Advisory Board, New World Vistas: Air and Space Power for the 21st Century (Washington, D.C.: U.S. Department of the Air Force, 30 January 1996), 50.

[25] Philip A. La Perla, Creating Information Knowledgeable Leaders Through Information Operations Education (Carlisle Barracks, PA: U.S. Army War College, July 1997), 1.

[26] Ibid.

[27] Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (New York: Little, Brown and Company, 1993), 146.

[28] Sullivan and Coroalles, 18.

[29] Naval Postgraduate School, "Information Warfare & Information Operations,"; available from <http://www.nps.navy.mil/~iwag>; Internet; accessed 13 March 1998.

[30] President William J. Clinton, "State of the Union Address," January 1997.

[31] Amy Harmon, "Software Jobs Go Begging, Threatening Technology Boom," New York Times, 13 January 1998, sec. A, p. 1.

BIBLIOGRAPHY

Correll, John T. "War in Cyberspace." Air Force Magazine, January 1998, 33-36.

Geppert, Linda and William Sweet. "Technology 1998." Spectrum, January 1998, 19-103.

Metz, Steven. Strategic Horizons: The Military Implications of Alternative Futures. Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 7 March 1997.

Petersen, John L. The Road to 2015. Corte Madera, CA: Waite Group Press, 1994.

President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructure. Washington, D.C.: President's Commission on Critical Infrastructure Protection, 13 October 1997.

Reimer, Dennis J. Army Vision 2010. Washington, D.C.: Department of the Army, 1996.

Shalikashvili, John M. Joint Vision 2010. Washington, D.C.: Chairman of the Joint Chiefs of Staff, 1996.

Sullivan, Gordon R., and Anthony M. Coroalles. The Army in the Information Age. Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 31 March 1995.

Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Little, Brown and Company, 1993.

U.S. Department of Defense. Defense 97. Alexandria, VA: American Forces Information Service, no. 6, 1997.

U.S. Department of the Army. Information Operations. FM 100-6. Washington, D.C.: U.S. Department of the Army, 27 August 1996.

U.S. Department of the Army, The Annual Report on The Army After Next Project, (Washington, D.C.: U.S. Department of the Army, July 1997), A-1.