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.

INFORMATION OPERATIONS AND ASYMMETRIC WARFARE... ARE WE READY?

BY

LIEUTENANT COLONEL LaWARREN V. PATTERSON
United States Army

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

USAWC CLASS OF 2002

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

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS AND ASYMMETRIC WARFARE...ARE WE READY?

by

LTC LaWarren V. Patterson
United States Army

COL Richard Jones
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

ABSTRACT

AUTHOR: LTC LaWarren V. Patterson

TITLE: Information Operations and Asymmetric Warfare…Are We Ready?

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES:29 CLASSIFICATION: Unclassified

Events of Sept 11th, 2001 have made clear one inescapable fact. Because of rapid advances in technology, particularly in the information arena, global communications now enable us to hear and see first hand issues, events and concerns from around the world. These in turn raise passions and compel people to rethink their own closely held beliefs, prejudices and hatreds, and in some cases morphing into actions such as espionage, sabotage or terrorism. Information Operations and future Asymmetric Warfare will have a major impact on the U.S. Army's ability to remain a viable warfighting entity as well as our simple survivability against future adversaries. Currently, the Army's Field Manual FM 100-6 (dated August 1996) is the most up-to-date guide on Information Operations available to the rank and file field soldier and leader. While at the same time, the Army's newest doctrinal publications, FM-1 and FM 3-0, address the Army's future in terms of who we are, what we do, how we do it today, tomorrow, jointly and within the full spectrum of operations that is the asymmetric warfare environment. It is, therefore, tantamount that our policies and future Army vision ensure Information Operations as a tool against asymmetric warfare remain on the forefront of Army strategic planning.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to thank my Project Advisor COL Richard Jones, USAF, for his time and patience in working with and guiding me through the completion of this research project. Also Ms. Bobbi Norcross from the Library's Computer Lab, who always provided superb assistance (with a smile) no matter how busy she was. I would also like to thank LTC Bob Ferrell and LTC Gil Griffin, my two best friends and fellow students here at the U.S. Army War College. Without their support and uplift when I needed it, this project would still be in my desk drawer and written in stubby pencil.

INFORMATION OPERATIONS AND ASYMMETRIC WARFARE...ARE WE READY?

Dr. Nicholas Negroponte, well-known professor and Founding Director of MIT's renowned Media Lab said it best, "computing isn't about computers anymore, it's about living. The giant central computer, the so-called mainframe has been almost universally replaced by personal computers. The nation-state itself is subject to tremendous change and globalization. Governments fifty years from now will be both larger and smaller. The forces of nationalism make it too easy to be cynical and dismiss any broad-stroke attempt at world unification. But in the digital world, previously impossible solutions become viable." [1]

The end of the Cold War changed the alliances and geopolitical dynamics of international relations, causing a rise in regional instabilities. These changes, combined with the proliferation of Information Age technology, have made high-technology weapons, electronic warfare (EW) equipment, reconnaissance, intelligence, surveillance, and target acquisition (RISTA), and information system elements more easily available to any country or organization around the world. Because of the perishable nature of information, commanders must understand the fluid nature of Information Operations

In the last 21 years, we have undergone a revolution in computers and Information Systems that has evolved faster than any other medium associated with our daily lives. The computer and associated information exchange systems have gone from the stand alone personal device, to what was five years ago a new catch phrase, "network centric," to where we are today, "Global Centric" or the Global Information Grid (GIG). It is now possible for a small dedicated C2 cell in an otherwise unsophisticated organization to create a temporary knowledge-based advantage over a militarily superior force, which can be translated into a military advantage. In the area of Information Operations, one must assume that any adversary can attain some level of parity with friendly forces. It is because of this global link-up that now, more than ever, we must be clear on where we stand in providing the best possible information systems for our Army, the DoD and other local, state and federal agencies. We must do this while simultaneously protecting ourselves from those that would seek to do harm to our Information Operations infrastructure through Asymmetric Warfare.

WHAT IS INFORMATION OPERATIONS?:

Information Operations are those actions taken to affect adversary information and information systems while defending one's own information and information systems. This includes the use of psychological operations, deception, jamming, and computer network attack and defense.[2]

In today's Information age, the U.S. is clearly in the lead in developing and exploiting cutting edge information technology and all its inherent potential. Our economy, social and civil infrastructures, local, state and federal governments have all become dependent on real time rapid and accurate communications. Concurrently, we exercise extraordinary influence around the world through our immense media, commercial and entertainment industries. Conversely, the U.S. is affected by similar influences outside its borders. The Global Information Infrastructure (GII), which electronically links individuals and organizations around the world, is characterized by an ever growing merger of civilian and military information networks and technologies.

Simultaneously, most if not all military operations take place within the Global Information Environment (GIE) which is pervasive in its presence and influence on how we conduct day-to-day business. Current and emerging technologies can bring any military operation directly into the homes and offices of a global audience in real or near real time without the benefit of de-coders or filters. With such easy access to national or global networks, suppression, control or censorship may not be realistic or desirable.[3]

As technology enables increasing numbers of individuals, organizations and nation states to be linked to the world through the GIE, these same players can be expected to eventually attempt to read, manipulate and control the content and flow of information contained within the Military Information Environment (MIE). These players and potential adversaries (in some cases current allies and some no doubt supported by non-friendly nation states) will seek to gain advantages in the GIE and MIE by employing battle space systems or any means at their disposal.

WHAT IS ASYMMETRIC WARFARE?:

Asymmetric Warfare is acting, thinking or organizing differently than the opponent in order to maximize one's own advantages or exploit an opponent's weakness. It comes from one force deploying new capabilities that the opponent force does not perceive or understand. It's conventional capabilities that counter or overmatch the capabilities of its opponent, or capabilities that represent totally new methods of attack or defense...or a combination of these[4].

Asymmetric warfare on U.S. soil is not new. In King Philip's War (1675-1676), the New England Indians abandoned their traditional restraints and prepared to wage war against all colonists regardless of their status as innocent civilian or combatant. King Philip's method of attacking the normally larger British forces by using smaller, more mobile forces, taking advantage of terrain and using ambush tactics would be successful in the Indian Campaigns for the next 140 years. The British forces were slow to react opting instead to continue using their normal formations and massing their fires against an enemy that became increasingly harder to see.

Indians in the Southern plains disrupted American efforts in the West by turning the once held in awe American telegraph system against U.S. forces. By the early 1800s, the Apache Indians had studied and learned the function of the telegraph system. When preparing for war, they would cut the lines and remove sections or simply replace a smaller section of wire with rawhide so that it appeared to be intact. This historical example was the preview of things to come under the auspices of cyber attacks.[5]

FM 100-6 cites several other interesting historical perspectives regarding Information Operations and early Asymmetric Warfare on the battlefield:

Example 1.

> One of the earlier applications of Asymmetric C2 Warfare was demonstrated during the American Civil War. From the beginning, telegraph lines became an important target of cavalry raiding parties from both sides. Since the Union forces were more extensively equipped with telegraphic systems, they were more vulnerable. This vulnerability was exploited by Confederate troops. Among the more innovative soldiers were the telegraphers attached to Confederate cavalry commands. These specialists, who were also qualified as flagmen, rode in the lead as Confederate cavalry units raided Union territory. They switched military traffic to the wrong destinations, transmitted false orders to the headquarters of Union commanders, and cast suspicion upon all orders that came by wire. When they had finished the job, they cut all the wire in sight and took home with them as much as they could roll up in a hurry.[6]

Example 2.

> In 1944, at the battle of Arnhem, the British First Airborne Division landed with the wrong radio crystals. They could not communicate with the outside, not even to their relief column at Nijmegen, a few miles away. They were isolated, under attack by superior numbers and surprised at being dropped where they were not supposed to be. During the entire multi-day battle, members of the Dutch resistance in Arnhem were routinely talking to their counterparts in Nijmegen by telephone, because the national telephone system had not been taken down. It never occurred to a single paratrooper to knock on the door of a house and call Nijmegen, because the battlefield had been defined outside the civilian infrastructure. The Dutch underground assumed the paratroopers were talking by radio, and paratroopers had never thought about using the civilian infrastructure.[7]

The Cyber threat now facing the U.S. is equally compelling and risks both the effectiveness of U.S. forces on the battlefield and the safety of private and government systems throughout the United States. Past JCS exercises such as Eligible Receiver and Zenith Star highlighted just how susceptible our command and control networks are to attack. Adversaries will use both old and new technologies to their advantage. A key example was the Chechen's use of Commercial Off-the-shelf (COTs) scanners and radios to intercept Russian communications. We can expect future adversaries to also attempt to acquire more advanced technology such as Global Positioning Systems (GPS) jammers to degrade our precision strike capability. U.S. intelligence sources site some 30 nations that have developed aggressive computer warfare programs.[8] In light of our military being so dependent on Information technology, this would be a prime asymmetric warfare target.

CURRENT INFORMATION OPERATIONS POLICIES:

JOINT PUBLICATION 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS

In March 1999, DoD reported that it detected roughly 80-100 "cyber incidents" on its computer systems on a daily basis. In calendar year 1999, there were more than 20,000 cyber attacks and approximately 14,000 attacks in the first seven months of Calendar Year 2000.[9] Fortunately, to help mitigate the effects of these "intrusions," DoD and the Joint Staff developed Joint Pub 3-13. Published in October 1998 under the direction of General Shelton, it provides the warfighter with the basic principles and Rules of Engagement to stop the enemy whose weapon of choice is bits and bytes, not bullets. Under JP 3-13, Information Operations cover the full spectrum of conflict from peace to crisis to war back to peace. Fueling JP 3-13 was also the growth to commercial industry and our ties to industry through network and global centric systems. Elements of industrial power can and will quickly transition into combat capability. Just like the airplane, Information Operations was first envisioned for commercial use but quickly developed as a combat weapon of choice. Under JP 3-13, DoD ensures Information Operations are a key part of its exercises and all contingency planning. Additionally, the U.S. military works with its allies to ensure joint and combined operations include, when feasible, Information Operations.

CLINGER-COHEN ACT OF 1996

This act assigned to the various Federal Department's Chief Information Officers (CIO) the responsibility to "ensure that the information security policies, procedures, and practices of the executive agency are adequate." Section 2224 of Title 10 of the U.S. Code mandated that the DoD CIO presents to Congress an Information Assurance Annual Report.

PRESIDENTIAL DECISION DIRECTIVE (PDD) 63-

This Presidential Directive dated 22 May 1998 and entitled, "Critical Infrastructure Protection," was built on the recommendations of the President's Commission on Critical Infrastructure Protection and sets a goal of reliable, interconnected, and secure information infrastructure by the year 2003, and significantly increased security to government systems by the year 2000. PDD 63 addressed the cyber and physical vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats. PDD 63 established new structures to deal with this important challenge. These new entities include:

A National Coordinator, whose scope includes internal infrastructure as well as foreign terrorism and threats of domestic mass destruction.

The *National Infrastructure Protection Center* (NIPC), located with and under the purview of the FBI, it brings together representatives of DoD, United States Secret Service (USSS), Energy, Transportation, the Intelligence Community and private sector in an unprecedented attempt at information sharing and quick resolution to major incidents.

Information Sharing and Analysis Centers, modeled after the Centers for Disease Control and are set up by the private sector in cooperation with the federal government.

National Infrastructure Assurance Council, whose members are drawn from private sector leaders and local/state officials to provide guidance to the policy formulation of a National plan.

The National Critical Infrastructure Assurance Office, which supports the National Coordinator's office along with government agencies and private sector in developing a national plan. PDD 63 is the culmination of a methodical, concentrated interagency effort to evaluate and ensure the security of the United States' increasingly vulnerable and interconnected infrastructures.

WHERE WE ARE TODAY:

The DoD's Information Operations mission is immense. In 1999, it was second only to Y2K in priority. Today it is DoD's top priority. At last count, the DoD had roughly 1.5 million desktop computers in its inventory. These computers combine to make up 20,000 Wide Area and Local Area Networks (W/LANs) of which 2,000 are considered critical to DoD's wide ranging missions.[10] Everything that occurs in a theater of operations is potentially subject to instantaneous scrutiny. Adversaries posture in hopes of causing reactions in the press without taking any real actions or risks. This can influence strategic decision makers and the direction, range and duration of operations by all involved.

We are the most studied military in the world. Foreign states have regular military features and even journals (such as the Russian Foreign Military Review) dedicated to the study and assessment of our military force structure, doctrine, operational concepts and capabilities. Many of us have at one time or another even accessed Army field manuals and joint pubs from the Internet (some of the input for this SRP is a prime example). In April 2001, the Center for Army Lessons Learned recorded 5, 464 hits on its website from Europe and another 2, 015 hits on its website from Asia. These were merely seekers of information and not individuals out to do harm. However, attackers, viruses and hackers are an annoyance that come with the technology of computers, and the combination of all three along with other activities could seriously disrupt the Army's daily business processes and its ability to carry out its assigned missions.

Many readings suggest terrorists are increasing their use of commercial Information Systems (INFOSYS) attacks. The terrorists' actions range from unauthorized access to using computer bulletin boards in order to pass intelligence and technical data across global borders. Even Drug Cartels are taking advantage of the possibilities that are offered by Information Systems. For relatively low cost, these drug entrepreneurs can acquire the capability to strike from a distance their enemy's commercial, security and Information systems infrastructure while enjoying anonymity and safety.

Individuals with legitimate access to a system can pose the greatest threat by far and the most difficult one from which to defend. Whether recruited or self-motivated, the individual insider has access to systems normally protected against attack. While an insider can attack a system at almost any time, it is most vulnerable during design, production transport and maintenance.

On the battlefield, a maneuvering forces' dependence on an extensive and in some cases a very fragile communications network (usually a combination of tactical, strategic and in many cases commercial links) presents a vulnerability that beckon exploitation. Like other major users of Information Systems, the U.S. Army relies on elements of the Information Infrastructure it does not control. Examples include integration and use of U.S. commercial and host nation Public Switched Networks (PSN) and telegraph systems; commercial satellite systems such as Intelligence Satellites (INTELSAT) and International Maritime Satellites (INMARSAT); commercially developed software applications; commercial and international news media; and public accessed data bases and bulletin boards. The cumulative effects of the integration of these systems can combine to create a target rich environment. Lucrative targets include vital Signal Nodes, Command Posts (CPs), radar stations and air defense centers. Commanders at the tactical, operational and strategic level as well as National leaders face major challenges in dealing with and attempting to anticipate the effects of the impact of global visibility of military operations.

U.S. Army units follow a general pattern during force-projection operations. Commanders require up-front signal support planning and continuous, detailed Intelligence Preparation of the Battlefield (IPB), to include an understanding of how the adversary uses information. Because of the fluid nature of force projection, national and joint intelligence systems must continually monitor and assess the effectiveness of Information Operations and act or react to potential dangers. To ensure effective integration of Information Operations, component commanders must tailor forces early, based of course upon the mission assigned by the combatant commander or Joint Forces Commander and available resources.

FM-3.0, "Operations," published in June 2001, is the Army's most recent doctrinal attempt at outlining the future of warfighting. As such, it has dedicated an entire chapter to the discussion of Information Operations and the Information Environment. Chapter 11 points out that the value of Information Operations is not measured in how well it affects the transmission of enemy data, but rather how well it effects the outcome of the mission.

To be successful at Information Operations, leaders must understand its effects on the local population, local political leaders and displaced persons. This requires thorough IPB. This would include such tidbits as enemy capabilities, decision making styles and what information systems the enemy has at his/her disposal. It would also consider other areas such as the media, local attitudes, economy, demographics and personalities of those living in the Area of Operations. [11]

As with any Battlefield Operating System, the desired effects of Information Operations are to destroy, degrade, disrupt, deny, deceive, exploit and influence the enemy. Depth and simultaneous attack will enable the commander to directly influence the enemy throughout the width, height and depth of his battle space, to strike, then to rapidly defeat the enemy. By massing the effects of conventional fires and integrating Information Operations designed to blind, demoralize and defeat the enemy, concurrent with rapid combined arms ground and air maneuver, a larger and less agile enemy force can be quickly and decisively defeated.

The global visibility of operations impacts a command's combat power by either enhancing or degrading soldier morale. Soldier spirit and perseverance, the will to win and dedication to the cause and devotion to fellow soldiers and the unit can be rapidly undermined. Bad news, misinterpretation and inaccurate information impact families and communities as well as soldiers, affecting their morale and commitment to the objective at hand and potentially undermining the critically important human dimensions.[12] Where the use of force is restricted or is not a viable option, Information Operations can influence attitudes, reduce commitment to an enemy's cause and make it clear our willingness to use force without actually doing so. Information Operations used this way could allow friendly forces to accomplish missions much faster with fewer casualties.

In a recent Washington Times article, William Hawkins, a National Security Senior Fellow at the U.S. Business and Industry Educational Foundation pointed out that terrorism and guerrilla warfare are asymmetric strategies that the U.S. has faced before. Those that are militarily weak but politically ambitious usually wage this kind of war. Mr. Hawkins singled out Mao Tse-tung as one of the best modern day practitioners of guerrilla and asymmetric warfare. This approach was the first phase in what would turn out to be a long protracted war pitting Mao's Communist insurgents against the Nationalist Chinese Government. As the war dragged on, the Nationalist troops became more and more disillusioned and demoralized. As they weakened, Mao's troops gained strength and confidence, until they were able to gain ground from which to build a strong base to launch strikes at the heart of the enemy...its will. [13]

The fight for the future makes daily headlines. Information Operations in an asymmetric environment is proving difficult...but not insurmountable. The deep dynamic guiding current think tank analysis is that the information revolution favors the rise of network forms of organizations.[14] The rise of networks means that power is migrating to non-state actors, because they are able to organize into sprawling multinational networks. This implies that future conflicts will be increasingly waged by "networks" perhaps more than by hierarchal organizations. It also means that whoever masters the network stands to gain the advantage.

David Ronfeldt and John Arquilla, authors of "Networks, Netwars and the Fight for the future," wrote extensively about networks. Regarding networks, some hold out the promise of reshaping specific sectors of society, as in the advent of the "electronic democracy" and a global "civil society." Most people might hold out hope for the emergence of a new form of organization to be led by "good guys" who do the right thing. Unfortunately, history does not support this contention. The cutting edge of new forms of technology is more often than not found among malcontents, ne'er-to-do-wells and clever opportunists, all eager to take advantage of new ways to maneuver, exploit and dominate.

The spread of networks and conducting information operations in an asymmetric environment clearly entails some new risks and dangers. It can be used to generate threats to freedom and privacy. New methods for surveillance, monitoring and tracking are being developed. Critical national infrastructures for power, telecommunications and transportation, as well as crucial commercial databases and information systems for finance and health, remain vulnerable to computer hackers and cyber terrorists. A growing digital divide between the information haves and have nots portends a new set of social inequities and create fertile ground for those who wish to take advantage.

Information Operations in an Asymmetric environment is not likely to be a passing fancy. As the information revolution spreads and deepens around the world, instances of netwars will proliferate across the spectrum of conflict. So will the sophistication and the arsenal of techniques that different groups can muster. At present, the rise of netwars extends from the fact that the world system is in a turbulent, susceptible transition from the modern era, whose climax was reached at the end of the cold war to an era that is yet to be aptly named. Netwars, because of dependency on networks, is facilitated by the radical increases in global and transnational connectivity, as well as from the growing opportunities for increased connectivity from another sense…the ability of outsiders to gain access to each other and even for insiders to be secreted within an organization or sector of society.[15]

The established norm of behavior used to be that terrorists groups would announce their threats and rush to take credit for their actions. In this way, their existence and their objectives would be as widely known as possible. A new trend is for terrorists not to take responsibility for their actions. The destruction, killing or maiming of targets is sufficient to the cause. Eschewing responsibility also avoids the prospect of retaliation, as occurred with the United States bombing of Libya in 1986 in retaliation for the bombing attack on a German pub frequented by U.S. soldiers. However, not taking credit does not necessarily avoid retaliation (as seen by the response to the September 11th 2001 attacks). The trend to avoid responsibility only makes it more difficult to track terrorist organizations, to trace terrorists' acts and to bring those responsible to justice.

As for the United States and its friends and allies, one challenge will be to learn to network better with each other. Some of this is already going on in terms of intelligence sharing, but much more must be done to build a globally operational counterterrorist network. In terms of doctrine, the al-Qaeda network seems to have a grasp of the nonlinear nature of the battle space and of the value of attack from multiple directions by dispersed small units. If the attacks of September 11th were indeed perpetrated by the al-Qaeda organization, its first campaign was no doubt the bombing of the Khobar Towers in Saudi Arabia in 1996, followed by a sharp shift to Africa with the embassy bombing in 1998. In between and since, there have been a number of other skirmishes in far-flung locales. Thus Mr. Bin Laden and his cohorts appear to have developed a swarm like doctrine that features a campaign of episodic, pulsing attacks by various nodes of his network.

Bin Laden also appears to be mapping out a strategy similar to that of Mao. Striking at the enemy's will to fight. He has made it clear that his aim is to drive the U.S. out of the Middle East and overthrow those governments he sees as corrupt puppets of the U.S. In his mind, if his calculations are right, then a decadent America would be displayed to the world as a super power without the stomach for a long fight. This in turn would embolden others who want the same thing as Bin Laden to join al Qaeda and support the fight.[16]

There are good reasons Bin Laden thinks his strategy will work. He has good empirical data. On 3 October 1993, a force of 100 Army Rangers and Delta Force commandos fought a battle with several thousand Somali militia, including identified al-Qaeda members. Eighteen Americans were killed and the world watched as U.S. service members' bodies were dragged through the streets of Mogadishu. It became apparent that Americans could no longer stomach the thought of casualties. If the death of 18 Americans chased the United States out of Somalia, how far would the U.S. retreat if thousands died?

Terrorists aren't the only ones looking closely at the strategy of striking at American resolve. In their widely read 1999 book, "Unrestricted Warfare," Chinese Colonels Qiao Liang and Wang Xiangsui wrote, "Viewed from the performance of the U.S. military in Somalia, where they were at a loss when they encountered Aideed's forces, the most modern military force does not have the ability to control public clamor and cannot deal with an opponent who does things in an unconventional manner."

Indeed this is a key issue to ponder. However, there is one important fact that makes the Somali mission different from our War on Terrorism taking shape in Afghanistan...American resolve. Clear U.S. objectives and public support for the Somali mission were never fully developed. Americans were anxious to pull their young men and women out of harms way in a conflict they neither agreed with nor supported. Conversely, the terrorists' attacks of September 11th took place on U.S. soil, was unprovoked and resulted in the deaths of thousands of innocent civilians. America's resolve appears to be steadfast. This could very well turn out to have been a gross miscalculation on the part of Bin Laden and the al Qaeda organization.

Yet interestingly enough, our unequaled use of air power in recent conflicts is seen by some as a superb asymmetrical warfare tool in the likes of guerrilla warfare. It is meant to weaken the enemy's will to resist the ground campaign, which will ultimately determine the outcome of the war. In Afghanistan, the Taliban's air defense system was rendered operationally combat ineffective early in the campaign. This gave U.S. troops the ability to strike when and where we wanted, conduct recon probes and airlift troops and supplies. The difference between winning and losing is the ability to impose the kind of political outcome that supports the nation's war aims.

The United States has made a point that the attacks on New York and Washington, D.C. were 'acts of war" against not only America but also the civilized world, and American public opinion has been quickly galvanized by the rebirth of the Pearl Harbor metaphor as a symbol of victimization. Justly so, the mass murder of thousands of civilians can only reinforce feelings of anger and indignation. However, against the doctrine used by al-Qaeda outlined in the previous paragraph, the U.S. has seemingly little defense. Some defensive measures such as an increase in "force protection" posture have been pursued and missile attacks on Afghanistan and the Sudan in 1998 suggest that the offensive part of U.S. doctrine is based on aging notions of strategic bombardment.

Fortunately, that was then...this is now. If one looks deeper at U.S. strategy being used in Afghanistan today, you would quickly discover that strategic bombing is only a small part of our offensive strategy. The President and his Cabinet are bringing to bear all components of National Power to include Diplomatic, Information, Economic and Military as well as extensive use (albeit expensive) of precision guided smart bombs, coalition special and conventional forces and indigenous troops. This combination of tangible and intangible forces has created a potent offensive mix in fighting terrorism in the asymmetric arena.

One of the greatest challenges in countering asymmetric threats in the realm of Information Operations is that borders have become meaningless to anyone operating in a virtual world. Even if great diligence was taken in the effort to remove vulnerabilities, it would be almost impossible to eliminate them entirely because attack tools, networks and network control systems are in a constant state of evolution.

As new technologies develop so too will new attack tools and mechanisms. As a result, the Army will have to set procedures in place to allow security initiatives to evolve to deal with new threats as they arise.

In a resource limited environment, conscious decisions must be made as to where scarce resources should be allocated to manage the risk to the Army. This risk management/assessment approach must not only clearly understand the threat and vulnerabilities but the impact on trade-offs and solutions. Therefore, a balance of investment made in the three areas of people, operations and technology will allow the Army to get the best return on its dollars. What makes our investment in the Information Operations arena even more pressing is the Global Information Grid (GIG).

The GIG (as defined by ASD (C3I)) is a globally interconnected, end to end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. The GIG not only serves the warfighter's needs for Information Superiority but also addresses the critical concerns of frequency spectrum and information infrastructure management.

The GIG is not just a combat tool, but also provides benefits and capabilities in the areas of logistics, computing services, communications, network operations and information management. The GIG is a constantly evolving entity as technologies, policies and capabilities are developed to take advantage of its vast potential.[17] The GIG is just one example, albeit a major example, of the emerging technologies and capabilities that Information Operations have to offer. The mission and vision for Information Operations have a strong link to supporting National Defense and is therefore tantamount to our National Interests.

The first critical step in protecting Information Operations in an Asymmetric environment (or any environment for that matter) is to identify specific threats current and future. Threats can range from the adversary's direct overt and covert actions, to individuals and organizations seeking to exploit military INFOSYS. The fluid porous nature of the MIE makes it difficult to protect INFOSYS from possible attacks. Therefore, intelligence provides commanders the necessary information to conduct risk assessments and develop risk management options to protect vital C2 components and capabilities. The risk assessment is not a finished document, but a continuous process that is constantly updated to reflect changes in the operating environment, technology and threat acquisitions.

LAND INFORMATION WARFARE ACTIVITY:

The challenge for commanders in the 21st Century is to operate effectively in a dynamic joint and multinational environment against a wide array of asymmetric threats. Maintaining the information high ground helps commanders meet that challenge. As full dimensional operations evolve, information and Information Operations become increasingly important to Army operations as the Army executes missions to deter conflict, to compel opponents, to reassure allies and friends and to provide domestic support.

AR 520-20 established the Land Information Warfare Activity (LIWA) to integrate OPSEC, military deception, PSYOP, EW and physical destruction to support Information Operations and C2 Warfare. LIWA coordinates multi-disciplined intelligence and other support for operations planning and execution, to include C2 Warfare database support, HUMINT, CI and TECHINT. LIWA is electronically connected with other national, DoD, joint and service IW facilities.

LIWA has been specifically designed to provide tailored support to the land component commands. LIWA's purpose is to provide commanders with technical expertise that is not resident on the command's general and special staff and to provide responsive technical interfaces with other commands, service components and joint information centers. LIWA is the designated Army operational focal point and Army executive agent for Information Operations.

ENDS, WAYS & MEANS:

As with any strategy development, particularly at the strategic level, the development of ends, ways and means is important to ensure we are on path to the desired end state. The ends, ways and means outlined below focus on the areas of operations, people and technology as a possible answer to our success in future Information Operations and Asymmetric Warfare.

ENDS:

Provide in a secure fashion, the right information, at the right time and place for the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks, effectively and efficiently.

WAYS:

Effective operational policies and doctrine.
Appropriate technology, tools and materials.
A corps of professionals educated and trained in Information Operations and Asymmetric Warfare
Continuous monitoring and assessment of threats, vulnerabilities and readiness postures.
The ability to quickly and efficiently implement agency wide security measures to limit damage when threatened.
Appropriate management and oversight.

MEANS:

Influence strategic planning and align Information Operations and Asymmetric Warfare doctrine to mission plans. Promote strategic planning as the basis for investing in Information Operations development. Develop partnerships with strategic commanders to help them see, understand and formulate planning that leverages the potential of Information Operations to revolutionize military operations which in turn will plant the seed for the growth of doctrine, policies and procedures at the strategic warfigther level and below.

Improve base level infrastructure. The Army's base level communications and computing infrastructure needs to be upgraded. Inconsistencies in technical and management procedures and capabilities complicate Information Operations planning and implementation. Even though efforts have been made to improve bandwidth, interoperability and value added services, tactical links need to be upgraded. Tactical information systems must be fully digitized and capable of transmitting graphics such as maps and other images to the warfighters (based on my own personal experiences, Europe based Communications units are feeling the pain from this).

Continue to train and certify all Army network managers, operators, systems administrators, and all personnel (right down to the user in the foxhole) involved in Information Operations. Review and create (as/when needed) military and civilian MOS related career fields to ensure that an adequate population of trained and ready warfighters is always on hand to support whatever missions may arise. We must also work to attract the best and brightest of our young people coming out of University level computer schools.

Influence and participate in operational exercises and demonstrations. This foresees the DoD growing into an all encompassing joint and defense wide environment which will lay the foundation for incorporating options and programs and bringing new capabilities to the field (where they are welcomed with open arms by the warfighters). Continue to use such spring board venues as Advance Technology Demonstrations, Advanced Warfighting experiments and other front end processes and assessment activities. These activities help thrust to the forefront Information Superiority and Information Operations in support of better mission performance across DoD and the Army.

Build a framework to determine the value of information. Our military capabilities are heavily dependent on solid reliable and focused information. The value of information is a primary discriminator in Information Operations protection strategies that focus on priority targets. This strategy requires developing and applying knowledge and tools for helping to determine the value of information to missions and tasks. This approach will help reduce the over abundance of information and enable the Army and DoD to treat information as a commodity.

Defense in depth is the strategy that DoD is pursuing to ensure success in both cyber warfare and other types of warfare that are dependent on Information Operations. Critical to the Army's ability to conduct warfare, Information Operations is the accepted responsibility of all modern warfighters. Because of the universal nature of the GIG, a risk assumed by anyone at any level is a risk assumed by all. Therefore, Information Operations is necessary at all levels. Through a structured and deliberate risk analysis process, Army leaders can make effective risk management decisions on how to counter enemy Information Operations measures in an asymmetric environment. The target for networks includes data, voice, wireless (pages and cellular) and tactical networks that support both operational and strategic missions. Again, these networks can be both Army (DoD) owned and operated or provided through leased lines.

Tactics used to defend these networks and infrastructures include the use of multiple and redundant data paths to allow more than one available alternative physical route for data transmission. The applicable technologies are monitoring and management tools, intrusion detections systems (IDS), encryptions of data and other anti-tamper mechanisms.

The market for encryption hardware and software is rapidly expanding. The U.S. is the primary developer and manufacturer of sophisticated encryption products, but overseas competitors are closing the gap. Encryption hardware and software products electronically encode data for security purposes. Governments, financial institutions and corporations routinely rely upon encrypted communications to conduct their daily business. So do individuals and groups that are hostile towards the National Security interest of the United States. For this reason, the unregulated export of sophisticated encryption products raises public safety and national security issues.

U.S. manufacturers complain that current export regulations prevent American producers from competing effectively in overseas markets. The regulatory prohibitions coupled with time line and reporting requirements render technically superior U.S. products non-competitive. [18]

If parties hostile to the United States have access to strong encryption products, not only can they hide their illicit activities, they might corrupt Defense Information, compromise military systems or interfere with military missions and operations. For this reason, DoD is concerned about the proliferation of strong encryption systems abroad.

Two legislative initiatives that seek to respond to industries' encryption export concerns are H.R. 850, the Security and Freedom Through Encryption (SAFE) act of 1999 sponsored by Representative Goodlatte (R-VA) and S. 789, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) act of 1999 sponsored by Senator McCain (R-AZ). Each represents unique legislation that removes encryption export control from the regulatory framework that currently governs the export of dual-use systems.

Both the Goodlatte and the McCain bills permit the unregulated export of strong encryption technologies within the very near future. However, neither bill sufficiently resolves the national security and public safety issues raised by the unregulated export and proliferation of strong encryption products.

THE FUTURE:

The Cyber battlefield is real. It's a place where computers are used instead of guns, data packets instead of bullets, and firewalls are used instead of barbed wire. Those that are still mired in fighting another "Desert Storm" or want to continue to live in the comfortable past of a largely bi-polar, superpower driven global situation may be in for a rude awakening as the nature of asymmetric conflict unfolds in the coming decade. There are few, if any countries that can militarily challenge the U.S. in open combat at the present time. Some seemingly astute assessments would suggest that China may become a future adversary with the industrial and conventional military power to eventually confront the U.S. and her allies, but they also point out that this capability is still evolving and that it may take China a minimum of three to five years or more to become a major threat to the United States and overall world stability.[19]

The future holds both opportunity and challenge for us regarding Information Operations and Asymmetric Warfare. Developing and fielding the right force mix in the face of continued technological advantages is clearly a monumental challenge. We must focus our energies on developing a Full Spectrum capability. As such, increasing our dependence on electronic and computer systems for managing the fight will move even more combat situations into the Information Operations environment.

The DoD policies and procedures currently in place are clearly taking us in the direction we need to go in regarding Information Operations for the first part of the 21st Century and up through 2015. At the same time we must be forever mindful that today's globalization of systems and networks creates a new dimension for warfare. The adversary can be a lone hacker either out for a thrill or with a grudge against the U.S. The new warfighter must become tomorrow's Cyber Warrior with the prerequisite technical and non-traditional skill sets required.

The literature regarding Information Operations in an asymmetric environment offers some interesting insights into our struggle with al-Qaeda and the conduct of our first major conflict of the millennium. Al-Qaeda seems to hold the advantage at the social and doctrinal levels and apparently in the organizational domain as well. For the United States and its allies, there is much room for improvement...most at the organizational and doctrinal levels. Simply put, the United States and its allies must build its own networks and learn to swarm the enemy in order to keep it on the run and pinned down until it can be destroyed. The United States and its allies must also seize the initiative including applying pressure on any states that harbor terrorists. To be sure, the real work needs to be done in developing an innovative concept of operations and building the right kinds of networks to carry off a swarming campaign against networked terrorists. For at its heart, Information Operations and Asymmetric Warfare are far more about organization and doctrine than about technology.

In less than one generation, our nation has experienced a profound transformation. The information revolution and the introduction of the computer into virtually every dimension of our society has changed how our economy works, how we provide for our national security and how we structure our everyday lives. New advancements in information systems technologies have given us limitless new possibilities for learning and creating, increasing the safety of our families and communities and building a new era of prosperity.

Yet, this new age of promise carries with it peril. Whether we are simply turning on the lights in our homes, boarding a plane or summoning help for a family member who has fallen ill, we are relying on one or more elaborate computer driven systems. Similarly, many of our most critical defense systems rely on commercial power, communications and transportation. All these systems are vulnerable to intrusion and destruction. Indeed, those who seek to challenge us may now prefer to attack these computer based systems rather than face us on the battlefield where America has an overwhelming preponderance of forces. Where once our opponents relied exclusively on bombs and bullets, hostile powers and terrorists can now turn a laptop computer into a weapon capable of doing enormous damage. If we are to continue to enjoy the benefits of the Information Age, preserve our security and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack.

SUMMARY:

Information Operations has emerged as a critical component of the Army's operational readiness, providing the means to detect, react, restore and deter intrusions or attacks from the outside or from within. Today we stand ready to handle the brunt of these Asymmetric attacks. However, Information Operation challenges still remain. The primary one is for the U.S. and specifically our military to be able to keep pace with rapidly evolving technologies. Related to this challenge is the need to keep personnel current with the new technologies and understanding them enough to be able to defend against threat initiatives. While technology will be critical to achieving greater operational agility and precision lethality, the human dimension of war will also take on increased importance. The soldier will remain the centerpiece of Army formations, and as the complexity of operations increases, well-trained disciplined soldiers and of course leaders will become ever more important. [20]

Information technology can help reduce but will not eliminate uncertainty on the future battlefield. It does however, give commanders windows of opportunity that can help them seize the initiative. Technologically assisted situational understanding of the battlefield may tempt some senior leaders to micromanage their subordinates' actions. This is not new; the telegraph and the command helicopter of Vietnam War fame created similar situations and tensions between senior and subordinate commanders.[21] Current and future commanders need to develop command styles that will exploit information technology while at the same time allowing subordinate commanders the authority as well as autonomy to accomplish their mission. Our Army leadership must continue to address vulnerabilities and the complexities of the issues related to Information Operations in an Asymmetric environment. Our success in this area will be our continued investment in operations, people and technology.

WORD COUNT = 7,313

ENDNOTES

[1] Nicholas Negroponte, Being Digital (New York: Vintage Books, 1995), 230

[2] Department of the Army, Information Operations, Field Manual 100-6 (Washington, D.C.: U.S. Department of the Army, 27 August 1996), glossary-7

[3] Ibid.,1-2

[4] Ike Skelton, Congressman, "Lessons for Asymmetric Conflicts," Military Review (September- October 2001): 23.

[5] Ibid., 26

[6] Department of the Army, Information Operations, FM 100-6, 6-3

[7] Ibid., 5-5

[8] Skelton, "Lessons for Asymmetric Conflict," 26

[9] Jim Garamone, "Joint Staff Releases Information Operations Doctrine," Defense Link, American Forces Press 10 March 1999; available from http://www.defenselink.mil/news/Mar1999/n03101999-9903106.html>; Internet; accessed 28 September 2001

[10] Department of Defense, Chief Information Officer Annual Information Assurance Report (Washington, D.C.: Department of Defense, FY 2000), 10

[11] Department of the Army, Operations, Field Manual 3.0 (Washington, D.C.: U.S. Department of the Army, 14 June 2001), 11-16 through 11-17

[12] Department of the Army, Information Operations, FM 100-6, 1-9

[13] William R. Hawkins, "U.S. advantage In Asymmetrical Warfare," The Washington Times 14 November 2001; available from <http://www.asp.washtimes.com> ; internet; accessed 14 November 2001

[14] David Ronfeldt and John Arquilla, "Networks, Netwars, and the Fight for the Future," First Monday on Line 10 October 2001; available from <http://www.firstmonday.org/issues/issue6-ronfeldt/index.html>; Internet; accessed 29 October 2001

[15] Ibid., 4

[16] Hawkins, 1

[17] Department of Defense, Chief Information Officer Annual Information Assurance Report ,18

[18] Department of Defense, Chief Information Officer Annual Information Assurance Report (Washington, D.C. : Department of Defense, FY 1999), 78-80

[19] Clark L. Staten, “Asymmetric Warfare, The Evolution and De-evolution of Terrorism; The Coming Challenge,” 27 April 1998; available from <http://www.emergency.com/asymetrc.htm>; Internet; accessed 29 October 2001

[20] Department of the Army, The Army Field Manual 1 (Washington, D.C.: U.S. Department of the Army, 14 June 2001), 36

[21] Department of the Army, Operations, FM 3.0, 11-24

BIBLIOGRAPHY

Geramone, Jim. "Joint Staff Releases Information Operations Doctrine." Defense Link, American Forces Press 10 March 1999. Available from <http://www.defenselink.mil/news/Mar1999/no3101999-9903106.html>. Internet. Accessed 28 September 2001

Hawkins, William R. "U.S. Advantages In Asymmetrical Warfare." The Washiington Times 14 November 2001. Available from<http://www.asp.washtimes.com>. Internet. Accessed 14 November 2001.

Negroponte, Nicholas. Being Digital. New York, Vintage Press, 1995

Ronfeldt David and John Arquilla. "Networks, Netwars, and the Fight for the Future." First Monday on Line 10 October 2001. Available from http://www.firstmonday.org/issues/issue6-ronfeldt/index.html>. Internet. Accessed 29 October 2001

Skelton, Ike Congressman . "Lessons for Asymmetric Conflicts." Military Review (September-October 2001) 22-27

Staten, Clark L. "Asymmetric Warfare, the Evolution and De-evolution of Terrorism. The Coming Challenge." Available from http:// www.emergency.com/asymetc.htm>. Internet. Accessed 29 October 2001

U.S. Department of Defense. Chief Information Officer Annual Information Assurance Report. Washington, D.C.: U.S. Department of Defense, FY 2000.

U.S. Department of Defense. Chief Information Officer Annual Information Assurance Report. Washington, D.C.: U.S. Department of Defense, FY 1999.

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

U.S. Department of the Army. Operations. Field Manual 3.0. Washington, D.C.: U.S. Department of the Army, 14 June 2001.

U.S. Department of the Army. The Army. Field Manual 1. Washington, D.C.: U.S. Department of the Army, 14 June 2001.