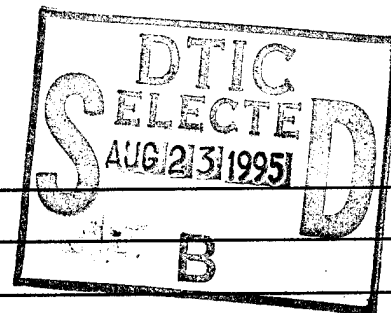


Unclassified
Security Classification This Page

REPORT DOCUMENTATION PAGE



1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): Achieving the Revolutionary Potential of Information Technology			
9. Personal Authors: Tony L. Cothron, Commander, U.S. Navy			
10. Type of Report: FINAL		11. Date of Report: 16 May 1995	
12. Page Count: 24			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: Revolution, Military Affairs, Leadership, Management, Intelligence, Command and Control, Information Technology			
15. Abstract: Information Age technology has great potential for improving regional CINCs and JTF staffs ability to plan and direct operations. But effective implementation of Information Technology will require a revolution in current policies, doctrine, practices and organizations. Examples of the types of changes required are examined, using commercial business, an historical analysis of command and control, recent initiatives in the U.S. Intelligence community and changes in U.S. Marine Corps doctrine. The examples highlight the need to focus on implementing reforms which liberate our personnel from Industrial Age management practices and empower them to contribute to a more effective military force.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
18. Abstract Security Classification: UNCLASSIFIED			
19. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
20. Telephone: 841-6457		21. Office Symbol: C	

Security Classification of This Page Unclassified

Naval War College
Newport, R.I.

Achieving the Revolutionary Potential
of Information Technology

by

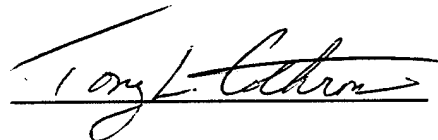
Tony L. Cothron

Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:



March 1996

Paper directed by
Captain D. Watson, U.S. Navy
Chairman, Joint Military Operations Department

19950822 121

"Warfare is primarily concerned with two sorts of activity - the delivering of energy and the communicating of information."¹

THE INFORMATION AGE AND REVOLUTION

Technology is pushing us faster and farther into what many are calling the "Information Age." Just as the development of mass production in the Industrial Revolution dramatically changed the world from an Agrarian-based economy, Information Technology has already begun to alter the way we live and work today. Central to the concept of the Information Age is that the primary economic asset is knowledge and is best represented by the "...ideas, skills and abilities of well-educated workers and leaders..."² The Information Age is a knowledge-based society -- a society linked through extensive information sharing networks, which Vice President Al Gore has labeled the "Information Super Highway."

Warfare is affected by Information Age technologies and some new applications were graphically demonstrated in the Gulf War in 1991. But the dramatic changes and challenges presented by warfare in the Information Age have only recently begun to be identified as a new "revolution in military affairs"³ (RMA) (see appendix 1). The focus of most current literature on the RMA and Information Technology is on the potential of technical capabilities such as "brilliant" weapons, attacks against enemy information networks or near-continuous surveillance of enemy forces. But this focus

☒	
☐	
☐	
by Godes	
and/or	
Dist	Special
A-1	

overlooks the heart of the problem: effective implementation of Information Technology will require fundamental changes - a revolution by itself - in the way the U.S. military is organized and operated. A network-based military, using the tools of the Information Revolution, can achieve the faster operational decision cycle, with less forces and staffs, needed to respond to tomorrows threats and requirements. Creating such a military requires throwing out Industrial Age policies, organizations and work habits. It requires new management practices and leadership, a focus on improving processes, greater decentralization and an emphasis on individual initiative.

The best examples of what types of changes we should begin to implement come from the same arena that is providing us Information Technology -- the commercial world. But other examples can also be shown in military history and in changes which are occurring now in the U.S. military.

INFORMATION TECHNOLOGY AND ORGANIZATION IN BUSINESS

Perhaps the best and most well known symbol of the Information Age is Cable News Network (CNN). Created in only 374 days by Ted Turner, CNN not only revolutionized television news, but how people think about information. The idea of broadcasting the latest, news, every 30 minutes, 24 hours a day was literally laughed at in 1979 when Turner announced his plan.⁴ Today, the CNN concept of "instant" news and reporting is the standard by which information

dissemination is measured.

The success of CNN is a testament to the vision and personality instilled in the organization by Ted Turner. Quality advocate Tom Peters in his book Liberation Management, says "Turner doesn't believe in failure....He does believe in taking the initiative."⁵ Peters spent several days closely observing how CNN works and reports the network is a superb example of radical centralization and decentralization. Information Technology allows instant communication with "centralized" decision makers in Atlanta, but it is through the initiatives of individuals throughout a decentralized organization which provide the options for decision making. Workers at CNN must be proactive and able to deal with extraordinary ambiguity and chaos because being successful at CNN means "figuring out how to do it yourself."⁶

Peters' book is filled with stories of a dozen other companies which have reinvented themselves by demolishing outdated organizations and cultures. According to Peters', a willingness to share virtually everything with everybody inside and outside the organization, creating on-line data bases for use across functional lines and instilling an "e-mail ethos" of information exchange between all levels of organizations are key concepts for successful implementation of Information Age technology in today's business world.⁷

TECHNOLOGY IN MILITARY HISTORY

Examples of revolutions in military affairs have usually been associated with new weapons or technology, such as the atomic bomb, gunpowder, the submarine or the telegraph (see appendix 1). But as historian and command and control expert Martin Van Creveld clearly shows in his book Command in War, it is understanding the limitations of technology which often means the difference in success or failure.

Van Creveld's analysis of command and control in World War I points out the differences in how technology is used effectively. At the turn of the century, new inventions such as the telephone, radio and wider ("tactical") use of the telegraph led some theorists to believe tactical operations could be directed by general staffs using information supplied by technology. An example of this type of thinking can be seen in a statement by the German chief of staff, General Alfred von Schlieffen:

"...the modern Alexander will have the entire battlefield under his eyes on a map. From there he telephones inspiring words, receives the reports of army corps commanders, captive balloon, and dirigibles, which all along the front watch the enemy's movements and register his positions."

Schlieffen's replacement who directed the German WWI effort, Helmut von Moltke the younger, was to find the reality in 1914 did not meet such visionary expectations. A closer look at how each side used technology in WWI best shows the importance of limitations.

The Allied offensive at the Somme in 1916 is one of the greatest disasters in military history. The training, assembly and deployment of over 400,000 men went on for more than four months. Objectives for the highly centralized plan (contained in a 57 page

order) were based on engineering considerations, not on terrain or enemy disposition and tactics. Commanders, from the battalion level up, were forbidden to accompany their troops and were required to stay by their telephone booths to receive orders from higher headquarters. To provide higher headquarters a better picture of the battlefield, troops were required to attack the German front marching shoulder to shoulder, in waves of four to eight, a hundred yards apart, and were prohibited from offering assistance to other units. It is not surprising, given such rigid preclusion of initiative, that sixty thousand men were lost (20,00 killed) in the first day of the battle.⁹

Given the same technological backdrop, the German Army developed a different doctrine for command in warfare and demonstrated its potential during an offensive in 1918. The German principles were based upon greater independence for subordinate leaders and the employment of officers from the general staff as the "directed telescope"* of higher headquarters.¹⁰ This directed telescope concept helped to overcome the limitations of the telegraph system. The emphasis on initiative and independent action was emphasized in the German directive for the offensive which stated "...every attack offers the opportunity for free activity and decisive action at all levels down to the individual soldier."¹¹ The German general staff understood the limitations of control during the

* Any means outside of normal official channels to bring a commander information. Typically it involves trusted staff officers (liaison officers) who report directly or through some communications method.

chaos of battle and placed reliance on improvisation, momentum and speed over rigid plans. While the operation itself did not achieve the major victory which the Germans had hoped for, Van Creveld attributes that failure to strategic errors and the inability by the German General Staff to exploit the tactical success which German units did achieve during the battle.

Van Creveld describes command as "an endless quest for certainty..."¹². In his conclusion of Command in War he notes two basic ways to deal with uncertainty: decentralization and centralization. Throughout history, Van Creveld observes, those who raised decision thresholds and reduced initiative in a centralized approach to command, invariably reduced their chances of success on the battlefield.¹³

INFORMATION TECHNOLOGY TODAY

The technology which fueled the explosion of the INTERNET in the private world is at use today within the DOD. One of the examples below focuses on the U.S. Atlantic Command's use of technological and organizational improvements in the last few years to correct deficiencies in intelligence dissemination identified during Operation Desert Storm. The second looks at an intelligence dissemination system, INTELINK, which is based on a new concept in security.

Innovation and Total Quality at U.S. Atlantic Command

Between 1991 and 1994 when U.S. forces were deployed to Haiti in

Operation Uphold Democracy, a series of initiatives significantly improved USACOM's ability to provide intelligence support to a Joint Task Force. As described by Rear Admiral Tom Wilson, former ACOM Director of Intelligence, the initiatives fall into four major categories:

- * theater-level joint Tactics, Techniques and Procedures development
- * intelligence operations in joint exercises targeted at major failings
- * improved, flexible joint intelligence communications connectivity
- * training teams tailored for joint intelligence operations at JTF-level.¹⁴

RADM Wilson credits much of the success of intelligence in Haiti to the fact that the forces used a common TTP for intelligence. One which was familiar to all components based on use during three annual exercises (1992-94).

The third initiative, the ACOM intelligence network ("ACOM Net") was built around two key components. One, known today as the Joint Deployable Intelligence Support System (JDISS), was designed in the early 1990s at ACOM under the name LANTDIS. JDISS is now the joint standard for intelligence dissemination and several hundred systems are deployed throughout the world. JDISS is a UNIX workstation which provides three primary functions: e-mail (interactive with other JDISS or one way to any intelligence command); imagery dissemination (i.e. a "fax"); and remote access to intelligence or

message data bases. Much like a home PC dialing into the INTERNET, JDISS provides the intelligence analyst with the ability to "plug in" to the intelligence community's information super highway - the DoD Intelligence Information System (DODIIS). More of a network than a "system," DODIIS provides "on line" connectivity throughout the intelligence community and is available to many tactical units, via either JDISS or interoperable service systems.¹⁵

A second major part of ACOM's Intelligence network is video teleconferencing (VTC). Part of the Joint World-wide Intelligence Communication System (JWICS), the VTC network was extended "down" to all of the principle and warfighting components of ACOM, including afloat as well as shore-based units. Ten different sites (see appendix 2), ranging from Fort Bragg (18th ABC) to USS Mt Whitney (COMSECONDFLT) and USS Wasp (CJTF 185.1 and CJTF 120), were able to conduct briefing sessions for intelligence and operational planning and coordination using the ACOM VTC net. Using this system, the forced entry option of Uphold Democracy was briefed by Admiral Paul Miller (CINC USACOM) and each of his components commanders at their own locations, to President Clinton, SECDEF and the CJCS in the Pentagon on 17 September 1994. While video teleconference briefings are not a new concept, the fact that all component commanders could personally participate in such a presentation is likely a first and representative of where information technology is taking us.

During the deployment of forces into Haiti during September 1994, the ACOM Network amplified the "directed telescope" of ACOM

augmentees at the JTF and component level. The VTC network was on continuously and used by watch personnel, at all levels of command, to pass updates and answer queries throughout the day. All members of the network, including the National Military Joint Intelligence Center (NMJIC) could "listen in" on discussions between analysts. The VTC, along with JDISS e-mail, provided for an informal dialogue which substantially contributed to a common perspective and shared situational awareness.

While the development and deployment of a robust, flexible network for intelligence connectivity was important, the "network" would not have been nearly as successful without a key change in a long standing access policy and development of a field support team at the Atlantic Intelligence Command (AIC). The policy change consisted of granting access to the ACOM message data base to any JDISS user in the ACOM theater. Previously, individuals outside of the staff and AIC could only access messages addressed to their unit. With the policy change, timely direct access to summary analysis from national agencies was provided to all intelligence personnel in the theater. More importantly, it gave the commands greater confidence that they had full access to all relevant intelligence and it did so without inundating commands with information.

The development of the AIC Field Support Team was accomplished through an eighteen month Total Quality Leadership (TQL) process. The AIC effort began in late 1992 as an initial TQL study on the problem of augmentation. The perceived problem with augmentation

was its enormous cost to the organization. But the "data" developed by a Process Action Team (PAT) indicated augmentation was only taking up 5% of the command's manpower. The real problem, identified by the PAT, was the lack of a clear process and (from the supported command's point of view) the lack of trained personnel as augmentees. The team's solution was to carve out 15% of the command to train for, coordinate and respond to augmentation and training requests. Enacted through a major command reorganization, the resulting Field Support Directorate and its three Field Support Teams was tested during exercise Agile Provider 94. The teams played a major role in training and augmenting Uphold Democracy JTF intelligence personnel. A key element in each Field Support team was a high degree of proficiency in Information Technology systems such as JDISS.¹⁶

INTELINK - Revolution in National Intelligence Dissemination

The second example of Information Age technology in intelligence is newer and has yet to be tested in operations, but it also shows the potential for significant improvement through a revolutionary policy change.

In early 1994, and over the space of only 45 days, the U.S. intelligence community developed a worldwide intelligence information service, designated "INTELINK."¹⁷ A true multi-media system, INTELINK users can obtain text, graphics, imagery and even video without a key board, using the same Mosaic software developed and used to access the INTERNET's worldwide web. With the MOSAIC-

based software, INTELINK users can "point and click" to access information on Top Secret/SCI servers at over twenty-one different intelligence agencies.¹⁸

It's not the technology behind INTELINK which is revolutionary -- it is the change in policy allowing direct access to individual organizations data bases. Users can "click" directly from a server at the Central Intelligence Agency to the National Security Agency to the National Photographic Intelligence Center (NPIC) to a theater Joint Intelligence Center, all without having to use a separate password (or needing special training). The burden for security is placed upon individual commands who grant local access to the system and the commands placing products on the INTELINK servers. Essentially, INTELINK provides access to an electronic "on-line" library of finished intelligence -- the type which generally sits, unknown, unread and unused in classified vaults. Still being deployed, INTELINK will eventually be found as an application on all joint and most service intelligence systems.¹⁹

A secret-level version of INTELINK, named "C2I LINK," has been incorporated into the latest version of the Global Command and Control System (GCCS) and is being fielded at 38 sites this spring.²⁰ C2I Link will provide "point and click" access to information servers at the secret NOFORN level around the globe and connected to the Defense Information Systems Network (DISN). While C2I Link will have access to intelligence data bases, it is not just a source for information on the threat. Just as in a commercial INTERNET node, command users can set up any number of

types of files for access by any user on the network. As an example, Appendix 3 is information pulled over the INTERNET which provides an excellent overview of Operation Deny Flight, currently being conducted by NATO's Allied Forces South command.

THE BEGINNINGS OF NEW MILITARY DOCTRINES

In describing the need for a more flexible and modern Army in the Information Age, General Gordon Sullivan, Chief of Staff, states that tomorrow's force will be smaller, but only more capable, if it is "equipped with modern technology, is well-trained and led, uses up-to-date doctrine and has organizations that 'fit' its technology and doctrine." Although General Sullivan eloquently states the need and impetus for change, he is less clear on exactly how the Army will revolutionize its doctrine and organization. The U.S. Marine Corps may be leading the way in this area with a new command and control doctrine aimed at decentralizing decision making.

The new Marine Corps concept will be included in Marine officer basic school later this year. According to Major General Paul Van Riper, Assistant Chief of Staff for Command, Control, Communications, Computers and Intelligence (C4I), the curriculum will emphasize "adaptability, judgment gained from experience, initiative and...intuition."²¹ This new approach to command and control replaces the traditional method where a commander's staff developed alternative courses of action, a process described by Colonel Charles Lyman, director of C4I Resources Management

Division at USMC Headquarters, as "...methodical, analytical, and slow..."²² The Marine Corps' change in doctrinal emphasis is being complemented by the addition of improved communications for the battlefield which promises much greater capability for vertical and horizontal coordination of information and better situational awareness. But despite improvements in intelligence surveillance and advanced C4I capability, Major General Van Riper says that "...uncertainty will continue to be a fact of life on the modern battlefield, at all levels of conflict."²³ In the context of the examples we have looked at (CNN, WWI and the intelligence community) the Marine Corps' change would appear exactly what is required for success in the Information Age.

RECOMMENDATIONS AND CONCLUSIONS

The heart of Operational Art is communicating a "vision" of the operation for subordinate forces to execute. Through Information Technology, regional CINCs and Joint Task Force commanders and staffs can better coordinate, plan and communicate, thus aiding and more quickly achieving a concurrent "vision" of operations among the operational and supporting forces. As seen in the ACOM example, there is much that can be done by the regional CINCs, individually and as a team with JCS and other national level agencies, to foster revolutionary improvements. Some other possibilities include:

- Enable units to "plug in" to the global military network of GCCS and other joint/service information systems through use

of inexpensive modems and telephones. Ships, squadrons and companies and platoons must all be given equal access and empowered to use the network's resources as they best see fit. The cost of fielding new GCCS workstations is too prohibitive to reach "down" far enough to the real warfighters who are creating the tactical picture of the battlefield.

- Maximize use of on line bulletin boards, data bases and data files at unclassified and classified levels.

- Create permanent E-mail addresses (unclassified and secret) for all DOD personnel and key command positions (duty officers and crisis watch positions) and maintain a global "white pages" with names, organizations and billets. Provide training and encourage use of e-mail for correspondence. (Why are we still faxing between commands and then recreating graphic files and texts?)

- Development of doctrine should be aided through on-line collaboration between service and joint doctrine and training centers. Direct inputs and "lessons learned" from those conducting operations should occur electronically and through video teleconferencing.

- Initiate concurrent "virtual planning" (and training) by cross-theater and service teams. This could be the needed answer for successfully manning our growing list of JTF staffs. Service colleges should be included in this network.

There are two problems with the promise of Information Technology -- the advocates are too optimistic about its

achievements and the skeptics are too pessimistic about its faults. There will be problems as we develop a new way of doing business. "Micromanagement" by higher commands could increase through the use of Information Technologys, like VTC. But that problem is not a feature of advanced technology. It is a personality trait which must be overcome through training and leadership. Some personnel will also, invariably, misuse network-based information. But it is unlikely a squadron or ship will deploy itself based on network access to a deployment order sent by the Joint Staff to a regional CINC. More likely, that unit will hastily began the necessary preparations and be ready to immediately deploy when tasked through its chain of command.

Whether we like it or not, new technology will continue to appear within our forces. We can ignore most of it, concentrating on new weapons, or we can begin to make the necessary changes to create the modern military force the U.S. needs for the 21st century. Creating that force will, most of all, require a focus on creating organizations, doctrine and policies which liberate our superb work force from Industrial Age management practices and empower them to contribute to a more effective U.S. military.

ELEVEN RMAS SINCE THE 14TH CENTURY*

Infantry

c. 1340. Bowmen supplanted knights. Warriors became individually cheaper.

Artillery

c. 1420. Supplanted siege warfare. Expensive. Fostered nation state (could subdue castles quickly, gain wealth, afford more artillery, subdue more castles, and so on).

Sail & Shot

c. 1600. Light galleys supplanted by artillery-carrying sailing ships (heavy).

Fortress

Trace Italienne. Forts make comeback.

Gunpowder

c. 1600. Muskets can pierce armor plate. Linear tactics replace pikemen. Swedish military system (pike, musket, cavalry, artillery)

Napoleonic

c. 1800. *levee en masse*. Sufficient men to both siege & maneuver. Interchangeable equipment parts. Staff system.

Land Warfare

c. 1860. Rail + telegraph = positive C2 plus continuous campaigning. Rifling and machine gun lead to entrenching. Impact on maneuver tactics not appreciated fully, even after numerous disasters.

Naval

c. 1850. Metal hulled, steam/turbine engines, long-ranged rifled artillery. Submarine. Torpedo.

Interwar (Mechanization, Aviation, Information)

c. 1920. Blitzkrieg. Carrier aviation. Amphib. attack. Strategic bombing. Drove unique organizations & CONOPs

Nuclear

c. 1950 (including ICBM).

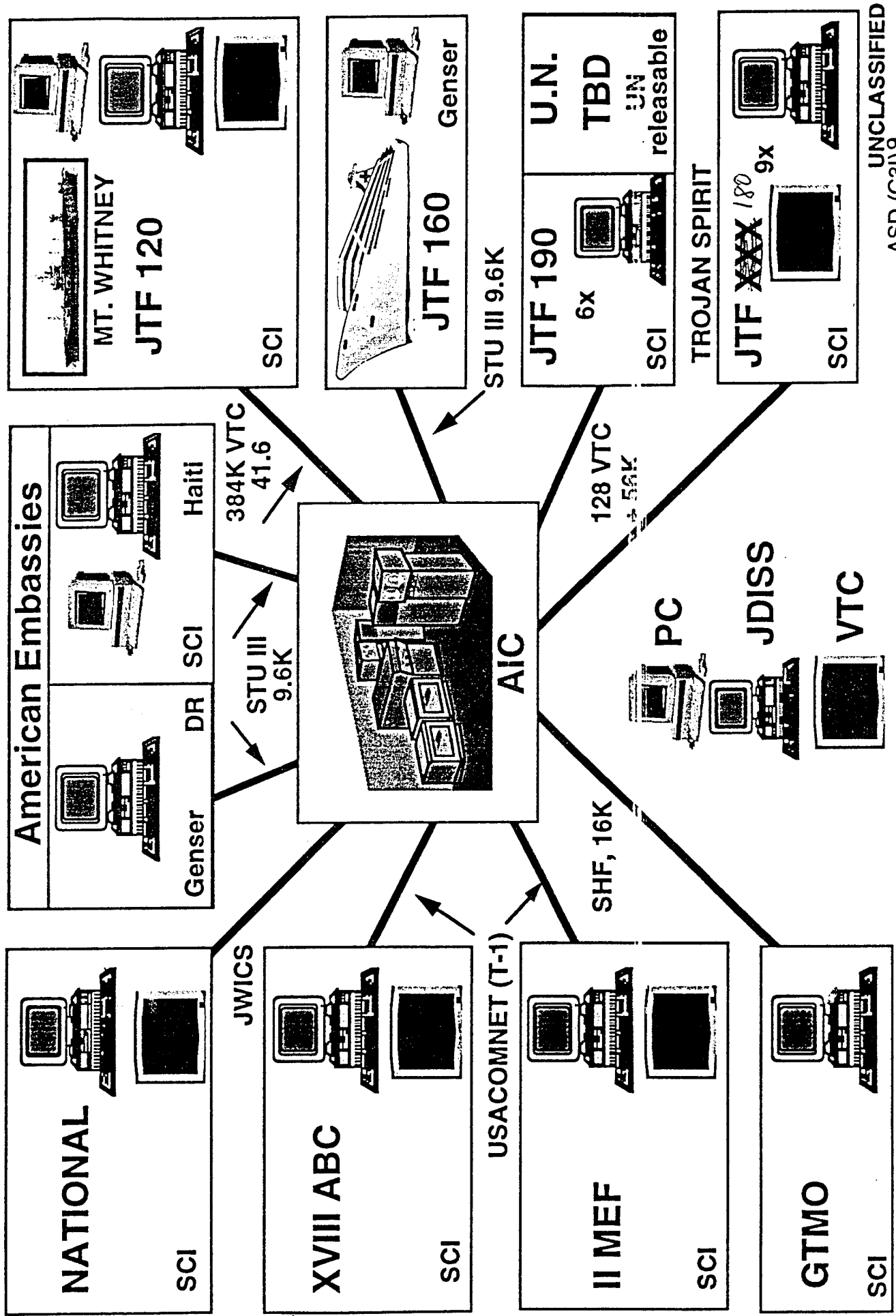
Microchip

c. 1990. IPP (Information, Penetration, Precision)

* 1-10: Krepinevich, *Cavalry to Computer*, *The National Interest*, Fall 1994, pp 30-42. #11: Barnett

UNCLASSIFIED

SYSTEMS ARCHITECTURE



NATO OPERATION DENY FLIGHT

MISSION:

The mission of NATO Operation DENY FLIGHT is threefold:

1. To conduct aerial monitoring and enforce compliance with UN Security Council Resolution (UNSCR) 816 which bans flights by fixed-wing and rotary-wing aircraft in the airspace of Bosnia-Herzegovina - "No-Fly Zone" (NFZ).
2. To provide protective air cover (CAS)) at the request of and control by UNPROFOR under the provisions of UNSCR 836 and 958.
3. To on order and in coordination with the UN, conduct approved air strikes against designated targets threatening the security of the UN safe areas of Bihac, Gorazde, Sarajevo, Srebrenica, Tuzla or Zepa.

ORGANIZATION:

The Supreme Allied Commander Europe (SACEUR) delegated authority for the implementation of Operation DENY FLIGHT to CINCSOUTH, Admiral Leighton W Smith Jr, U.S. Navy, with headquarters in Naples, Italy. He delegates control of the operation to the Commander, Allied Air Forces Southern Europe (COMAIRSOUTH) Lieutenant General Michael E. Ryan, U.S. Air Force, with headquarters in Naples. Operational control of day-to-day mission tasking is delegated to the Commander, 5th Allied Tactical Air Force, Lieutenant General Andrea Fornasiero, Italian Air Force, at Vicenza, Italy. Coordination between NATO and the UN has been arranged through an exchange of representatives between 5th ATAF and the UNPROFOR Headquarters in Zagreb and Sarajevo. These liaison officers ensure a continuous exchange of information between NATO and UNPROFOR.

PARTICIPATING FORCES:

Almost 4,500 personnel from 12 NATO countries -- Belgium, Canada, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, Turkey, the United Kingdom and the United States -- are deployed for this NATO operation. NATO aircraft are available at air bases in France, Germany, Greece, Italy, the United Kingdom or on carriers in the Adriatic.

France:

- 4 x Mirage F-1CR reconnaissance aircraft at Cervia AB,

- 6 x Italy.
- 6 x Jaguar ground attack aircraft (CAS) (on recall) at Cervia AB.
- 6 x Super Etendard fighter-bombers (CAS) on the aircraft carrier Foch (when in the Adriatic).
- 5 x Mirage 2000 ground attack aircraft (CAS)(plus 3 on recall) at Cervia AB.
- 1 x C-135 air-to-air refuelling aircraft at Istres, France.
- 1 x E-3F airborne early warning aircraft at Avord, France, or Trapani AB, Italy.

The Netherlands:

- 6 x F-16A fighter aircraft (NFZ) at Villafranca AB, Italy.
- 3 x F-16A ground attack aircraft (CAS)(plus 5 on recall) at Villafranca AB.
- 3 x F-16R reconnaissance aircraft (plus 1 on recall) at Villafranca AB.

Spain:

- 1 x CASA 212 support aircraft at Dal Molin Military Airport, Vicenza, Italy.
- 8 x F-18A fighter aircraft (NFZ) at Aviano AB, Italy.
- 2 x KC-130 air-to-air refuelling aircraft at Aviano AB.

Turkey:

- 8 x F-16C fighter aircraft (NFZ) (plus 10 on recall) at Ghedi AB, Italy.

United Kingdom:

- 6 x F-3 Tornado fighter aircraft (NFZ) at Gioia del Colle AB, Italy.
- 7 x Jaguar ground attack aircraft (CAS) (plus 3 on recall) at Gioia del Colle AB.
- 2 x Jaguar reconnaissance aircraft at Gioia del Colle AB.
- 6 x Sea Harrier dual-role capable aircraft (CAS/NFZ) on call on HMS Invincible (when in the Adriatic) .
- 2 x K-1 Tristar L-1011 air-to-air refuelling aircraft at Palermo, Sicily (Italy).

United States:

- 8 x USAF F - 15E (CAS) at Aviano AB. (On recall)
- 11 x USAF F-16C dual role capable aircraft (CAS/NFZ) (plus 1 on recall) at Aviano AB.
- 12 x USN F/A -18C dual role capable (CAS/NFZ) or F-14 fighter aircraft (NFZ) on call on the U.S. carrier when in Adriatic.
- 12 x USAF O/A-10 ground attack aircraft (CAS) at Aviano AB.
- 6 x USN F/A-18C or A-6E ground attack aircraft (CAS) on the U.S. carrier when in Adriatic.
- 3 x USAF EC-130 Airborne Battlefield Command and Control

- 2 x Centre aircraft (plus 2 on recall) at Aviano AB.
- 2 x USAF AC-130 Gunship aircraft (plus 2 on recall) at Brindisi AB, Italy.
- 10 x USAF KC-135 air-to-air refuelling aircraft at Pisa, Italy, and Istres, France.

NATO Airborne Early Warning Force aircraft:

- 8 x E-3A aircraft at Geilenkirchen, Germany; Trapani, Italy and Preveza, Greece.
- 2 x E-3D aircraft at Royal Air Force Station Waddington (UK), and forward operating bases at Aviano AB.

The French E-3F aircraft and those from the E-3A and E-3D Components of NATO's Airborne Early Warning Force (NAEWF) are supporting Operation DENY FLIGHT as well as the combined NATO/WEU Adriatic embargo enforcement Operation SHARP GUARD. The E-3A aircraft are flown by multi-national crews provided by 11 NATO nations.

The force is also supported by six USN EA-6Bs and six USAF EF-111A.

STATISTICS AS OF 05 APRIL 95:

Number of days since Op DENY FLIGHT Started = 724
 "No-Fly" Zone fighter sorties flown over Bosnia-Herzegovina
 = 18,673
 Close Air Support and Air Strike sorties over Bosnia-Herzegovina
 = 18,342
 Sorties by NAEW, tanker, reconnaissance and support aircraft
 = 17,428

HISTORY and SIGNIFICANT EVENTS

On 17 December 1994, a French Etendard IV P jet on a NATO reconnaissance flight over Bosnia-Herzegovina was hit by ground fire and returned safely to an airbase in Italy. The aircraft which had taken off from the French aircraft carrier Foch received tail damage. The pilot was not injured.

On 23 November 1994, following an attack the previous day on NATO aircraft by surface- to-air missiles, NATO reconnaissance aircraft were accompanied by escorts. The aircraft were illuminated by SAM radars, and in self defence attacked the SAM sites at Otoka and Dvor, firing anti-radiation "HARM" missiles. Later that same day, NATO carried out a strike against the Otoka SAM site, as it had been assessed as still posing a threat to

NATO aircraft.

On 21 November 1994, NATO aircraft attacked the Ubdina airfield in Serb-held Croatia. The air strike, conducted at the request of, and in close coordination with, UNPROFOR, was in response to attacks which had been launched from that airfield against targets in the Bihac area of Bosnia-Herzegovina in the previous few days. It was carried out under the authority of the North Atlantic Council and United Nations Security Council Resolution 958.

On 22 September 1994, following a Bosnian Serb attack against a French armoured personnel carrier (APC) near Sarajevo, NATO aircraft attacked a Bosnian Serb tank which was within the 20-kilometer exclusion zone around Sarajevo. The air strike was carried out at the request of UNPROFOR by a USAF OA-10 and two U.K. Jaguars operating in NATO Operation Deny Flight.

On 5 August 1994 the Bosnian Serb Army (BSA) seized a number of heavy weapons from the Ilidza Weapons Collection site in the Sarajevo Exclusion Zone, despite having been warned by UNPROFOR not to do so. At the request of UNPROFOR, NATO launched aircraft on the afternoon of 5 August to attack heavy weapons that were violating the Sarajevo Exclusion zone. Despite poor weather conditions the force, made up of Dutch, French, NATO, UK and US aircraft, were able to locate an M1S Tankbuster (a tracked 76mm anti-tank gun). This was attacked by two US A-10 aircraft who strafed it with 30mm ammunition. Following the air strike the BSA returned the heavy weapons they had taken.

On 22 April 1994 the NAC, responding to a request from the UN Secretary General, decided that the Bosnian Serb actions around the Gorazde safe area met the conditions identified by NATO on 2 August 1993 as grounds for air strikes. It required the Bosnian Serbs to immediately cease attacks against the safe area and to pull their forces back 3 km from the centre of the city by 0001 GMT on 24 April 1994 and from that time allow UNPROFOR and humanitarian assistance free access to the city. Additionally, it declared a 20 km military exclusion zone around Gorazde and required all Bosnian Serb heavy weapons to be withdrawn by 0001 GMT on 27 April 1994. As a result of UN and NATO cooperation, effective compliance with the NATO ultimatums occurred and air strikes were not required.

On 22 April 1994 the NAC decided that if the UN safe areas of Bihac, Srebrenica, Tuzla or Zepa were attacked by heavy weapons from any range or there was a concentration or movement of such weapons within 20 km of these areas then they would be declared military exclusion zones. NATO would back up such declarations with air power.

Notes

1. N.F. Dixon. On the Psychology of Military Incompetence (London: Jonathan Cape, 1976), p. 1.
2. Gordon R. Sullivan and James M. Dubik, War In the Information Age (Carlisle Barracks: U.S. Army Strategic Studies Institute, 1994), p. 1.
3. James R. FitzSimonds, "The Revolution In Military Affairs: Challenges for Defense Intelligence," Working Group on Intelligence Reform Papers, Washington, D.C. 1995, p.1
4. Thomas J. Peters, Liberation Management, Necessary Disorganization for the Nanosecond Nineties (New York: Alfred A. Knopf, Inc., 1992), p. 32
5. Ibid. p. 41.
6. Ibid. p. 39
7. Ibid. p. 122
8. Martin Van Creveld, Command in War (Cambridge, MA: Harvard University Press, 1985), p. 153.
9. Ibid. p. 156-168.
10. Ibid. p. 172.
11. Ibid. p. 174.
12. Ibid. p. 264.
13. Ibid. p. 274.
14. Thomas R. Wilson, "Joint Intelligence and UPHOLD DEMOCRACY." Joint Forces Quarterly, Spring 1995, p. 56.
15. Russel E. Myers, "Challenges to Defense Intelligence Information Systems Professional" American Intelligence Journal, Autumn/Winter, 1994, p. 45.
16. Wilson, p. 55-56.
17. Steven R. Schanzer, "INTELINK, An Information Strategy," American Intelligence Journal, Autumn/Winter 1994, p. 37.
18. Myers, p. 49.

19. Myers, p. 49.

20. Telephone conversation with Mr. Russ Myers, Chief, Information Technology, U.S. Atlantic Command, 17 April 1995.

21. Glenn W. Goodman, Jr., "The Synthesis of Uncertainty." Sea Power, April 1995, p. 75.

22. Ibid. p. 75.

23. Ibid. p. 75

Bibliography

- Barnett, Jeff. "The Revolution in Military Affairs." U.S. Office of Net Assessment Briefing, Washington: 1995.
- Dixon, N.F. On the Psychology of Military Incompetence. London: Jonathan Cape, 1976.
- Goodman, Glenn W. "The Synthesis of Uncertainty." Sea Power, April 1995.
- FitzSimonds, James R. "The Revolution in Military Affairs: Challenges for Defense Intelligence." Working Group on Intelligence Reform Papers, Washington: 1994.
- Myers, Russel E. "Challenges to Defense Intelligence Information Systems Professional." American Intelligence Journal, Autumn/Winter 1994.
- Owens, William. "System of Systems." U.S. Naval Institute Proceedings, May 1995.
- Peters, Thomas J. Liberation Management, Necessary Disorganization of the Nanosecond Nineties. New York: Alfred A. Knopf, Inc. 1992.
- Schanzer, Steven R. "INTELINK, An Information Strategy." American Intelligence Journal, Autumn/Winter 1994.
- Sullivan, Gordon R. and James M. Dubik. War in the Information Age. Carlisle Barracks: U.S. Army Strategic Studies Institute, 1994.
- U. S. Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations, Joint Pub 2.0. Washington: 1993.
- Van Creveld, Martin. Command in War. Cambridge, MA: Harvard University Press, 1985.
- Wilson, Thomas R. "Joint Intelligence and UPHOLD DEMOCRACY." Joint Forces Quarterly, Spring 1995.