UNCLASSIFIED

NAVAL WAR COLLEGE
Newport, R.I.

LEASHING THE HYDRA: CONTROL OF JOINT INTELLIGENCE ARCHITECTURES (U)

By

Michael W. Boardman

Lieutenant Colonel, United States Army

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

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 Army.

Signature: _____

13 ~~June~~ MAY 1997

Paper directed by CAPT George Jackson, USN
Chairman, Joint Military Operations Department

UNCLASSIFIED

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): Leashing the Hydra: Control of Joint Intelligence Architectures (U)	
9. Personal Authors: Michael W. Boardman, Lieutenant Colonel, United States Army	
10.Type of Report: FINAL	**11. Date of Report:** 19 May 1997
12.Page Count: 19	
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 or the Department of the Army.	
14. Ten key words that relate to your paper: Joint; Intelligence; Architecture; Technology; Information Management; Information Warfare; Desert Storm; Provide Comfort; Uphold Democracy; Joint Endeavor.	
15.Abstract: Modern joint intelligence architectures are extraordinarily complex creations. Information age technology has greatly increased their capability, but has simultaneously increased the difficulty of planning and managing them. The intelligence architectures in Desert Storm, and all United States joint operations since then, have reflected significant architectural problems, resulting in various forms of dysfunction or potential dysfunction, as a result of unanticipated or unmanageable complexity. Numerous initiatives throughout the Defense community are working to minimize these problems, but the rapidity of technological change continues to pose architectural challenges to intelligence planners and operators.	

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

Abstract of

LEASHING THE HYDRA: CONTROL OF JOINT INTELLIGENCE ARCHITECTURES

Modern joint intelligence architectures are extraordinarily complex creations. Information age technology has greatly increased their capability, but has simultaneously increased the difficulty of planning and managing them. The time-tested skills of common sense, tactical and operational finesse, and evaluation and interpretation that once sufficed for an intelligence officer are no longer sufficient; the intelligence state of the art now demands fluency in the realms of information processing, data communications and system design.

The complexity of the joint intelligence architecture created in Desert Storm generated many dysfunctions, which can also be seen in every joint operation since then. They stem from the explosion of technological capability and complexity. As intelligence architectures become more competent, they become harder to design, manage and troubleshoot.

Numerous initiatives throughout the Defense community are working to minimize this tendency, but the pace of technological change continues to generate new, unforeseen difficulties. American reliance on technology appears to be increasing, and this will generate difficulties in planning and managing joint intelligence architectures as fast as it increases capability, unless techniques are developed to better train and focus the intelligence architect.

I Introduction

Hydra: Gk. Myth. *A many-headed monster slain by Hercules.*[1]

Modern intelligence, particularly in the Joint environment, is an extraordinarily complex, detailed business, and it is growing more so every day. A "mature" Theater intelligence architecture—defined as all those moving parts necessary to define needs, collect information, analyze it, turn it into products that commanders need, when they need it, and then disseminate them to the far corners of the Theater—has hundreds, if not thousands, of highly interdependent elements, all working in a choreographed sequence of events. The design of this architecture is absolutely critical to its performance, because the efficiency of the joint theater intelligence system is related directly to the effectiveness of its design. Just as a poorly designed vehicle wastes fuel, runs inefficiently and requires constant tinkering, so a bad intelligence architecture wastes resources, is unresponsive to commander's needs, produces inaccurate and untimely intelligence, and resists adaptation to changing circumstances. A carefully crafted intelligence architecture is to the J2 what a well-tuned command and control system is to the J3.

The advent of the information age has the generated unprecedented challenges for intelligence planners and operations officers at every echelon: the hydra of technological complexity is growing heads faster than the same technology can be harnessed to simplify them. The skills of common sense, tactical finesse, evaluation and interpretation that once sufficed for an operational intelligence officer are now insufficient; the state of intelligence art now demands not only those basics, but fluency in the realms of

information processing, data communications, encryption, systems design. Intelligence architecture may well need to become an entire subspecialty within the intelligence profession. Without such specialists, the emerging intelligence architectures will be run-away engines without engineers. The joint intelligence community needs a race of architectural Hercules, to control rather than slay the Hydra, bending technological complexity to the will of its masters.

II Intelligence Without Architecture

Desert Shield/Storm illustrates the importance of architectural planning in joint intelligence. This was the largest joint intelligence endeavor since Vietnam, and arguably the most truly *Joint* since World War II. All services were totally engaged, as was the national intelligence community in the form of the CIA, the NSA and the DIA. Moreover, the controlling headquarters, CENTCOM, was joint, and in the post Goldwater-Nichols environment, it kept the respective Service headquarters in Washington DC genuinely at bay. Desert Storm was thus the first example of a deployed, theater-level, joint intelligence operating system since the Goldwater-Nichols reforms.

Desert Storm intelligence is also a landmark because it occurred in the first blush of the developing information revolution. Email, file transfer, digital imagery, broadcast information and extensive use of satellite technology all made their battlefield debut.[2]

---

[1] Webster's II, New Riverside University Dictionary. Boston: Houghton Mifflin, 1984.

[2] Special Operations Forces and some parts of XVIIIth Airborne Corps used some of this technology in Just Cause, but Desert Storm saw the first broad-scale, joint demonstration of information technologies for intelligence.

Each of the services brought an extensive array of intelligence collection, processing, and dissemination systems to the war, but CENTCOM had never developed an architecture to integrate it all. As the House Armed Services Committee noted in its 1993 report on intelligence successes and failures in Desert Storm, "At the time of the invasion, CENTCOM intelligence had. . . no joint intelligence architecture of substance to guide the buildup of in-theater intelligence capabilities."[3]

In the absence of a central architecture, each service wired together its own plan for intelligence operations. The result was a plethora of leading-edge technology systems in the theater, yielding better intelligence than ever before given to battlefield commanders, but at the joint/theater level, it became a hodge-podge architecture where joint interoperability occurred by happenstance, if at all. The observations in the following Assistant Secretary of Defense for C3I report are revealing:

> "The imagery dissemination business was even more chaotic than the RFI process. Every operational force that had an organic imagery dissemination capability brought it to the party. These imagery dissemination capabilities included the: Litton TDF, Laptop Imagery Transmission Equipment (LITE), PORTS, ICON, DVITS, Enhanced Tactical User's Terminal (ETUT), Tactical High Mobility Terminal (THMT) and Fleet Imagery Support Terminal (FIST). The TDF communicated using STU-III, KY58 and Tri-Service Tactical Digital Communications. The Navy forces afloat continued to use their FIST via the Fleet Broadcast SATCOM (FLTSAT) system. The Naval Intelligence Activity provided the LITE to the Marine forces as an operational prototype... it communicated using STI-III, tactical radio and STICS. The Army forces used the imagery dissemination capabilities of the ETUT and THMT via the FLTSAT. In addition to all of these, the DIA NMIST used the PORTS-1A/B via UHF SATCOM. Finally, USCENTCOM and their component command headquarters exchanged imagery with the ICON using STU-III and SHF SATCOM.[4]

---

[3] U.S. Congress, House of Representatives, Committee on Armed Services, Subcommittee on Oversight and Investigations, Intelligence Successes and Failures in Operations Desert Shield/Storm. Report (Washington: U.S. Govt. Print. Off., 1993), p. 1.

[4] Perspectives on C^{3}I Performance in Desert Shield/Desert Storm, (Washington: Mitre Corporation, 1991), p. A-12.

This report is highly revealing in two regards. First, it demonstrates the astonishing number of different systems brought to the Theater just for the one intelligence mission of imagery dissemination. Many of these systems were incompatible with the others, by virtue of different file formats, transmission formats or communications paths. As a result, each organization with one of these "toys" made its own arrangement with the organizations producing the imagery, and if your device was not compatible, you had to request the imagery in "hardcopy"—printed images, taking days or weeks. From the perspective of a joint intelligence architect, this situation was beyond management or repair.

Second, the reader is struck by the sheer number of acronymmed systems mentioned: 15, not counting generic "SATCOM. Each system had unique operational characteristics, specific communications parameters and distinct training and maintenance requirements. There were few, if any, intelligence officers in Theater broadly educated enough to make intelligent architectural decisions on so broad a scale. The result of the unplanned, uncoordinated proliferation of systems was architectural chaos.

Nor was the chaos limited only to imagery systems. Information architectures in general were subject to the same uncoordinated proliferation illustrated by imagery systems: "theater headquarters had a variety of incompatible ADP systems within and among the headquarters. As a result, horizontal message flows were difficult and may have adversely impacted joint/integrated air/land operations and planning."[5] In this case, information systems and intelligence were simultaneously beneficiaries and victims of exploding technology. Lacking architects to plan, and systems engineers to monitor, both systems expanded to the limits of Component Service capability.

Joint interoperability was not the only casualty. A cohesive architecture also considers personnel, training and maintenance requirements, as well as standardized techniques for things like readiness reporting and quality control. Clearly, these simply could not be evaluated, let alone managed, from the joint level under such circumstances.

III Since Desert Storm

With the problems of joint intelligence architecture so well recognized in Desert Storm, the intervening years have seen substantial progress, but the problem set has also continued to grow. In some ways, it appears more intractable than ever. It is not that the joint intelligence community cannot produce more, better, faster intelligence—it can. Nor that intelligence interoperability among services is worse—it has improved markedly since Desert Storm. What has grown harder in the intervening years is the same problem of mastering the hydra: gaining superiority in the planning, design, supervision and maintenance of a comprehensive joint intelligence operating system. If joint intelligence is a faster moving train now, the engineer is hanging on the caboose with a couple less fingers.

The root of the problem is the almost exponential growth of technological capability, and with it, complexity. The six years since Desert Storm have seen radical growth in the technology of information management, and "Information Supremacy" has become a base tenant of United States military strategy.[6] The means of intelligence

---

[5] Ibid., p. 50.

[6] "**Win the Information War**: The remarkable leverage attainable from modern reconnaissance, intelligence collection and analysis, and high speed data processing and transmission warrants special emphasis." National Military Strategy of the United States, Washington: The Joint Chiefs of Staff, 1995),

collection, processing and dissemination now are greatly improved over the Desert Storm era, but the speed of improvement is outrunning our ability to control it. Almost every technical improvement brings increased complexity to the architecture: more complex systems, more sophisticated automation, increasingly difficult maintenance, more communication demands, and a host of unforeseen interactions. As the architectures become more competent, they become harder to design, manage and troubleshoot.

This phenomenon can be seen in every joint or combined operation since Desert Storm. In Operation Provide Comfort 3 (Kurdish relief in Northern Iraq), the problem was training: matching the skills of joint personnel detailed to the headquarters with unfamiliar equipment. The combined headquarters operated with mostly detailed personnel on 6-8 month tours. Because the United States Air Force predominated in this operation, and because it was headquartered at the air base at Incirlik, Turkey, the intelligence architecture leaned heavily toward Air Force collection, processing and communication systems. But the mission called for a certain level of ground expertise, and many of the detailed personnel were Army.

Predictably, there was a large problem in training, maintenance and systems engineering; many Army personnel (and not a few Air Force also) were unfamiliar with the systems in use, and there was neither time nor facilities to properly train them. This shortfall was a major challenge in Combined Force intelligence operations.[7] In the days of typewriters, this problem would not have occurred, but those days are gone. We now

---

p. 15. See also the Chairman of the Joint Chiefs of Staff vision statement, Joint Vision 2010 (Washington: Chairman of the Joint Chiefs of Staff, undated), p. 16.

[7] Interview with COL David Piirto (USAF), former Deputy Chief of Staff for Intelligence (C-2), Combined Task Force Provide Comfort, at San Antonio, Texas: 2 May 1997. COL Piirto served in the CTF from September 1993 to February 1994.

have to deal with highly capable, specialized architectures that demand more in the way of personnel management and planning than ever before.

Operation Uphold Democracy (Haiti) appears at first glance to be an exception: by all accounts, the intelligence operations went very smoothly, demonstrating a coherent centrally planned intelligence architecture and effective joint management. Indeed, the OASDC3I assessment is conspicuous for the absence of many problems seen in Desert Storm.[8] But a careful reading of the Intelligence-related Issues section reveals hints of the very same problems that plagued Operation Provide Comfort:

> "Division-level collection managers familiar with Army tactical collection doctrine, systems and procedures operated at a significant disadvantage when thrust in a JTF role. Staff needed more instruction about available collection systems, especially non-Army systems and Army TENCAP systems. . .No suitable collection management courses were available to spin up the G2 staff before deploying for Operation Uphold Democracy."[9]

Suitable training was not available because most of the systems referred to were so new and sophisticated that the military training establishment had not caught up. Fielding state of the art intelligence systems is one thing, but fielding an entire *architecture* commensurate with those systems, to include trained and ready personnel, is quite another.

Despite some shortfalls, Operation Uphold Democracy was an extremely successful intelligence operation, but we should not infer that all the problems of architecture have therefore been solved. The successes in Uphold Democracy actually support the contention that *successful* intelligence architectures require extended,

---

[8] Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Intelligence Support Agency, Architectures Directorate, Operation Uphold Democracy: An Assessment of Intelligence and Communications Systems and Networks.Architectures, (Washington D.C.: 1995).

deliberate planning and preparation. Consider the following elements of JTF 180's success:

- The predominant element of JTF 180 was XVIIIth Airborne Corps, which had a long history of association with the controlling headquarters, USACOM. This history of exercise and coordination minimized interoperability problems.

- The JTF headquarters operated from the USS Mount Whitney, which provided exceptional intelligence communications and the core of a JTF analytical cell. The J2 staff was able to operate just offshore, close to the operation, but without having to build the intelligence command and control apparatus on the ground from nothing.

- XVIIIth Corp, the JTF staff and USACOM planned this operation, (in fits and starts) for over a year. Time allowed great attention to detail.

- Both the USACOM and XVIIIth Corps staffs put significant personnel resources against the architectural effort. The Corps dedicated a G2 Plans Lieutenant Colonel heavily to architectural planning for the whole planning period. Moreover, the Corps MI Brigade commander was an active advocate (and practitioner) of architectural thinking.[10]

The contrast of circumstances with Operation Desert Shield/Storm could not be greater. Where the CENTCOM staff was badly under strength in 1990[11], the XVIIIth Airborne Corps/JTF 120 intelligence staff was robust. Where CENTCOM was forced to react to events, building the joint intelligence architecture as quickly as possible, Operation Uphold Democracy was intensely planned and reviewed for over one year.

---

[9] Ibid., p. 5-13.

[10] My source for this information is personal experience; I was the Chief of XVIIIth Airborne Corps G2 Plans during the initial phase of the planning effort. I dedicated another Lieutenant Colonel who worked for me as a dedicated G2 planner and architect.

[11] "At the time of the Iraqi invasion, the CENTCOM/J2 organization was a mere shell. . . it did not possess the types or numbers of staff positions required to fulfill its wartime mission." U.S. Congress, House of Representatives, Committee on Armed Services, Subcommittee on Oversight and Investigations, Intelligence Successes and Failures in Operations Desert Shield/Storm, Report (Washington: U.S. Govt. Print. Off., 1993), p. 5.

The intelligence architects of Uphold Democracy corrected the problems of Desert Storm, in part at least, because they had the time and resources necessary to master the complexities of the operation.

Intelligence operations in Operation Joint Endeavor (Bosnia) experienced other aspects of the architectural issue. That operation was well planned in advance, and apparently quite successful, but it had to accommodate several elements not found in Uphold Democracy. For one, it was a much less familiar, cohesive organization; the G2 received large numbers of augmentees from outside the command at the last minute. Wearing its second hat as Task Force Eagle, the 1st Armored had to integrate numerous non-U.S. elements, including the Russian Brigade. Finally, the chains of command, supervision and higher supporting intelligence organizations were considerably more complicated than those in Uphold Democracy. These factors all combined to generate a number of serious architectural problems for the G2.

Chief among these was the gradual escalation of capability—a sort of "asset creep" in the division intelligence architecture. For the best of reasons, various "capabilities", in the form of systems, downlinks, and personnel, kept showing up to offer services in Tuzla. These were very difficult to decline: Some were sponsored by a higher commander or intelligence staff, to include the EUCOM J2 or the Joint Staff; some brought a mission essential state of the art or even prototype capability. Major General Nash, the 1st Armored Division Commander, was a voracious consumer of intelligence, and few G2's would want to admit, "I don't know, because I turned away (this or that) asset." In an atmosphere where casualty avoidance is paramount, no intelligence officer willingly declines additional capability.

As a result, the G2 section of the Division Main Command Post (CP) grew from the normal 5 vans and 4-6 other vehicles to a groaning 30-35 separate trucks, vans and assorted vehicles, sprouting untold antenna's and demanding many times the usual amount of electricity and other support.[12] Simply laying the electrical harness to safely power the whole net was a major electrical engineering challenge. 13-15 civilian contractors supported the operation, which grew to far and above the largest single element in the whole CP.

While this growth ultimately benefited the overall Division intelligence capability, it did present numerous challenges to the rest of the architecture. There was no organic expertise on how to coherently integrate all this capability electronically. As usual[13], a couple of smart noncommissioned officers and warrant officers, armed with a tool kit and lots of nerve, became the in-house "experts" on how to make one system talk to the rest. These individuals had no specific systems integration training, and they were extracted for this job from their other intelligence duties. In short, they were talented amateurs doing an additional duty. Such people are worth their weight in gold to a G2 or J2 in the field, but they are no substitute for a professionally trained system integration specialist.

Another potential difficulty inherent in the IFOR intelligence architecture never came up: movement. I asked LTC Patrick, in the event of a tactical need to move the G2 part of the CP, how long it would have taken, and who she had that was smart enough

---

[12] Interview with LTC Melissa Patrick, (US Army), former Assistant Chief of Staff for Intelligence G-2, 1st Armored Division, at Ft. Belvoir, VA: 6 May 1997. LTC Patrick is now commanding the INSCOM Support Battalion, Ft. Belvoir, VA.

[13] Both my experience and my research confirm that most military organizations do not have professional expertise assigned to accomplish this task of "system integration", i.e. adapting a pre-planned architecture to changes. The task usually devolves on the pair of smart individuals mentioned, assisted by

about the whole kluge to put it quickly back together. After a short pause, she replied, "Days... and nobody."[14]

The architecture was brittle. It's growth was neither uncontrolled nor accidental; the G2 accepted it for its enhanced capability, but at the same time accepted the risk of a tactical headquarters complex and cumbersome beyond anyone's ability to effectively maneuver.

Much of the intelligence technology first employed tactically in Desert Storm has matured, and it was used effectively in the Haitian and Bosnian operations. But Haiti demonstrates the price in planning time required to build a *controllable* architecture, and Bosnia shows that even the best planning may not avoid serious design problems. Technology in the intelligence field is advancing so rapidly that the concerns of a well founded architecture—functionality, controllability, sustainability, trainability—may be sacrificed to the single element of capability.

IV Improvements

The joint intelligence community is not blind to the problems of intelligence architecture. There are many efforts ongoing, which bear on one aspect of the issue or another, but none have so far genuinely mastered the problem.

Possibly, the most prominent effort to redress the problems of intelligence architectures is the Office of the Assistant Secretary of Defense for Command, Control

---

whatever contractor supports the affected system. While one may applaud this 'Yankee ingenuity', the approach is reaching its limits as the complexity of the electronic architectures grows.

[14] Interview with LTC Patrick.

and Communications: OASDC3I[15]. This office has the responsibility (among other things) to document and encourage architectural intelligence joint interoperability, and has started several initiatives concerning intelligence architectures. It founded the Command Intelligence Architecture Program (CIAP), intended to research and professionally document both the current and objective intelligence architectures of each Unified Command. Further, the CIAP identifies incompatibilities between the Commands and serves as a standard reference for planners and system developers to reach objective compatibility in the future. The individual Command Plans are painstakingly researched with the cooperation of the Command, and updated periodically. Prior to the CIAP, there was no architectural document standardized across the unified commands, and hence no way to easily identify similarities or incongruities. Now intelligence professionals can compare apples to apples. The CIAP has played a significant role in resolving joint intelligence compatibility issues.[16]

Another effort is the CHIP series: C4I Handbooks for Integrated Planning. Begun in 1986, the CHIP's are a comprehensive, classified series designed to "provide understanding of information, services and technology for the intelligence community."[17] They are updated periodically, and they are probably the best single reference available for information on architectural issues.

---

[15] Originally titled OADSC^{3}I (Command, Control, Communications and Intelligence), the mission was first expanded to include computers (C^{4}I), then expanded again in 1997 to include the mission areas of Reconnaissance and Surveillance.

[16] Interview with Mr. John Wyand, CIAP Program Manager, Architectures Directorate, C4ISR Integration Support Activity, OASDC3I, Washington: 6 May 97.

[17] C4I Handbook for Integrated Planning: National Intelligence Agencies and Organization. Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, C4I Integration Support Activity, Architectures Directorate, Integrated C4I Architectures Division. (Washington: 1996), p. iii.

The office also generates other architectural products, such as the assessment of intelligence and communications architectures in Operation Uphold Democracy (Haiti), referenced at footnote 8.

Another ongoing project of great promise is the development of software to help manage intelligence architectures. The office is sponsoring a contract to produce the Joint C4RSI Architecture Planning/Analysis System (JCAPS), a software application to provide analytical tools and a data repository for building and managing joint intelligence architectures.[18] If successful, this will be an important tool in every J2's repertoire of resources. It represents one of the best steps yet to use information technology for controlling the unintended problems of technological growth described in Sections II and III.

Another useful development, this one occurring without centralized guidance, is the publication of Tactics, Techniques and Procedures (TTP) manuals for J2 operations. Every geographically oriented Unified Command now has one. In each command, they detail how the command organizes and conducts intelligence operations—a sort of super SOP. Though not detailing the specific intelligence architecture in so great a detail as the CIAP, they document *how* the architectural elements work together in both deployed and non-deployed operations. In that sense, they function as an operator's manual for the joint intelligence operating system. If kept updated, they will help minimize the heavy impact of constant modernization and proliferation discussed earlier.[19]

---

[18] Ibid.

[19] For a detailed discussion of the role played by the USACOM TTP in the intelligence successes of Uphold Democracy, see Operation Uphold Democracy: An Assessment of Intelligence and Communications Systems and Networks, p. 5-20.

V Conclusions

How will the joint force of the near future deal with the dynamics of complexity and system proliferation? As seen, the entire joint intelligence community is struggling with the problem, and many solutions have come up, but it is certainly not clear that the solutions will even keep up with, let alone surpass, the accelerating pace of technological improvement, with its attendant growth in sophistication and complexity.

There is a crashing need for professional joint training on the topic of joint architectural development and management. While there exists abundant training on individual intelligence systems, and on whole subsystems, such as space, national sensors or the national cryptology program, I found no reference to any training program that addresses the problems of designing and managing *the whole, as an integrated operating system*. The OASDC3I Handbook for Integrated Planning: National Intelligence Agencies and Organizations does not address training, nor could its authors reference me to any.[20]

Occupational specialization is another possibility. All the services now train information systems specialists, but these tend to narrowly focus on information systems; the problem with intelligence architectures transcends mere automation. The joint intelligence architect must bridge all the other elements . The Army's Officer Personnel Management System Task Force XXI is considering a new officer specialty: Functional

[20] Interview with Mr. John Wyand. The Army intelligence training program at the US Army Intelligence Center trains company grade officers in managing tactical intelligence operating systems in the broadest sense, but focuses on the more narrow issue of collection management or the particulars of individual systems. There is no training at the Center addressing the issues discussed in this paper, and none at all focused on the field grade level of the problem. Interview with LTC Doug Phelps, Director of Training Developments, United States Army Intelligence Center, Fort Huachuca, AZ: 2 May 1997.

Area 30, Information Operations, which would include the functions of systems, intelligence and operations integration.[21] However, the proposal is not yet approved, and it remains to be seen how the concept will be fleshed out, if approved by the Army's Chief of Staff.

Civilian contractors are making an increasing contribution to the design and maintenance of intelligence systems; possibly, we may have to increase reliance on them. But this comes at a price: diminished flexibility in the force, dilution of unit integrity. Moreover, civilians are in no better position to correct the unresolved problems of intelligence architectures than uniformed personnel. No one has a monopoly on the answers yet.

One thing is clear: it will not get easier. In the American way of war, intelligence is highly dependent on technology, and accelerating technology is generating difficulties of management as fast as it creates new capability. If the hydra is allowed to grow heads faster than we can leash them, joint intelligence will continue to suffer unforeseen and unpredictable architectural deficiencies.

---

[21] "Option 3". Officer Personnel Management System XXI Task Force Briefing, (undated). < http://www.army.mil/opms/Brief.htm >, (8 May 1997).

Bibliography

Chairman of the Joint Chiefs of Staff. Joint Vision 2010. Washington, (undated).

Defense Intelligence Agency Joint Military Intelligence Training Center. An Intelligence Resource Manager's Guide, Ed. 1994. Washington: 1994.

Headquarters, United States European Command. Command Intelligence Architecture Program, Objective Architecture Document. ECJ2-P: 1992.

Interview with Lieutenant Colonel Melissa Patrick (US Army), former Assistant Chief of Staff for Intelligence G-2, 1st Armored Division, Fort Belvoir, VA: May 1997.

Interview with Lieutenant Colonel Doug Phelps, Director of Training Developments, United States Army Intelligence Center and Fort Huachuca, AZ: 2 May 1997.

Interview with Colonel David Piirto (US Air Force), former Deputy Chief of Staff for Intelligence (C-2), Combined Task Force Provide Comfort 3, at San Antonio, Texas: 2 May 1997.

Interview with Brigadier General Richard Quirk (US Army), Deputy Chief of Staff for Intelligence J-2, United States Southern Command, Quarry Heights, Panama: 2 May 1997.

Interview with Mr. John C. Wyand, Command Intelligence Architectures Program Manager, Architectures Directorate, C4ISR Integration Support Activity, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Washington: 6 May 1997.

Hura, Myron and Gary McLeod. Intelligence Support and Mission Planning for Autonomous Precision Guided Weapons. Santa Monica: Rand Corporation, 1993.

Mitre Corporation. Perspectives on C3I Performance in Desert Shield/Storm. Washington: 1991.

Officer Personnel Management System XXI Task Force Briefing. "Option 3" (undated). http://www.army.mil/opms/Brief.htm. (8 May 1997).

Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. C4I Integration Support Activity. Architectures Directorate. Integrated C4I Architectures Division. C4I Handbook for Integrated Planning: National Intelligence Agencies and Organizations. Washington: 1996.

Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. Intelligence Support Agency. Architectures Directorate. Operation Uphold Democracy. An Assessment of Intelligence and Communications Systems and Networks. Washington: 1995.

Office of the Joint Chiefs of Staff. National Military Strategy of the United States. Washington: 1995.

U.S. Congress. House of Representatives. Committee on Armed Services. Subcommittee on Oversight and Investigations. Intelligence Successes and Failures in Desert Storm/Shield. Report. Washington: U.S. Govt. Print. Off., 1993.

Webster's II, New Riverside University Dictionary. Boston: Houghton Mifflin, 1984.