NAVAL WAR COLLEGE
Newport, R.I.

NETWORK CENTRIC WARFARE IN OPERATION ALLIED FORCE: FUTURE PROMISE OR FUTURE PERIL?

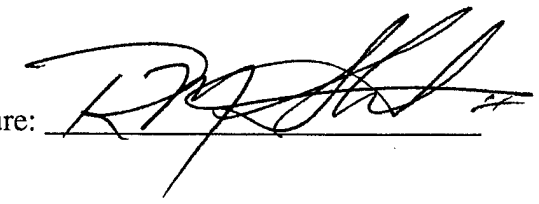
by

Robert M. Stuart II

Captain, United States Navy

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 Navy.

Signature: 

16 May 2000

John T. DuGene, CAPT, USN

12 A

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: NWC Code 1C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
NETWORK CENTRIC WARFARE IN OPERATION ALLIED FORCE: FUTURE PROMISE OR FUTURE PERIL? (U)

9. Personal Authors:
Robert M. Stuart II, Captain, U.S. Navy

10.Type of Report: FINAL

11. Date of Report: 16 May 2000

12.Page Count: 24

12A Paper Advisor (if any): CAPT John T. DuGene

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:

Network Centric Warfare, Operation ALLIED FORCE, unintended consequences, information interoperability shortfalls

15.Abstract:

Elements of Network Centric Warfare (NCW) had a significant impact on the Headquarters, U.S. European Command conduct and oversight of Operation ALLIED FORCE, the NATO combat operation conducted in and around the Serbian province of Kosovo from March to June 1999. A number of technological advances that constituted significant elements of NCW at the theater and operational level made conduct of Operation ALLIED FORCE unique. NCW connectivity brought with it a number of problem areas that, if unchecked or uncorrected, could adversely impact European theater operations in the future.

Theater access to real-time, full motion video surveillance of targets of interest, the reliance on reachback technology by the European theater intelligence community, daily reliance on VTC's to facilitate essential warfighting coordination and SIPRNET data sharing advances at HQ USEUCOM were all successes of NCW during ALLIED FORCE.

Despite these successes though, NCW in Kosovo was not a panacea for warfighting connectivity in a coalition setting. A major stumbling block was realized in the lack of U.S. and European information interoperability, as well as the potential for senior leaders inappropriately inserting themselves in tactical level decisions. The European Security and Defense Identity (ESDI) and Defense Capabilities Initiative (DCI) provide a starting point for NATO keeping up with the U.S. technologically, but if our European allies don't carry through, this "technology gap" will widen, threatening NATO cohesiveness.

16.Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461

20.Office Symbol: NWC Code 1C

Security Classification of This Page Unclassified

Abstract

Elements of Network Centric Warfare (NCW) had a significant impact on the Headquarters, U.S. European Command conduct and oversight of Operation ALLIED FORCE, the NATO combat operation conducted in and around the Serbian province of Kosovo from March to June 1999. A number of technological advances that constituted significant elements of NCW at the theater and operational level made conduct of Operation ALLIED FORCE unique. NCW connectivity brought with it a number of problem areas that, if unchecked or uncorrected, could adversely impact European theater operations in the future.

Theater access to real-time, full motion video surveillance of targets of interest, the reliance on reachback technology by the European theater intelligence community, daily reliance on VTC's to facilitate essential warfighting coordination and SIPRNET data sharing advances at HQ USEUCOM were all U.S. successes of NCW during ALLIED FORCE.

Despite these successes though, NCW in Kosovo was not a panacea for warfighting connectivity in a coalition setting. A major stumbling block was realized in the lack of U.S. and European information interoperability, as well as the potential for senior leaders inappropriately inserting themselves in tactical level decisions. The European Security and Defense Identity (ESDI) and Defense Capabilities Initiative (DCI) provide a starting point for NATO keeping up with the U.S. technologically, but if our European allies don't carry through, this "technology gap" will widen, threatening NATO cohesiveness.

TABLE OF CONTENTS

"If wise, a commander is able to recognize changing circumstances and to act expediently...If courageous he gains victory by seizing opportunity without hesitation."[1]

- Sun Tzu

Introduction

Elements of Network Centric Warfare (NCW) had a significant impact on the Headquarters, U.S. European Command (HQ USEUCOM) conduct and oversight of Operation ALLIED FORCE, the NATO combat operation conducted in and around the Serbian province of Kosovo from March to June 1999[†]. A number of technological advances that constituted significant elements of NCW at the theater and operational level made conduct of Operation ALLIED FORCE unique, and provide a glimpse into the "Revolution in Military Affairs" (RMA) of which NCW is an integral part. These advances impacted the operational level in such a way that they will unquestionably be built upon to provide a more robust capability when the next conflict of similar impact arises. Conversely, NCW connectivity brought with it a number of problem areas that, if unchecked or uncorrected, could adversely impact European theater operations in the future.

Thesis

Elements of NCW greatly assisted in the operational level conduct of Operation ALLIED FORCE, but some unintended consequences of NCW will imperil NATO effectiveness if not adequately addressed in the future.

[†] The author was assigned to Headquarters, U.S. European Command (HQ USEUCOM) Operations Directorate, Current Operations Division, Joint Reconnaissance Center from March 1997- February 2000.

Network Centric Warfare

In January 1998, Vice Admiral Arthur K. Cebrowski noted how "we are in the midst of a revolution in military affairs (RMA) unlike any seen since the Napoleonic Age, when France transformed warfare with the concept of *levée en masse*."[2] This RMA was brought on by the proliferation of information technology and computer connectivity as manifested today in the extensive availability of Internet access. The RMA's military embodiment has been coined Network Centric Warfare (NCW), and it has been the subject of extensive discussion within the past few years. NCW encompasses a myriad of computer networking and information sharing technologies that has been described as:

> "...an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization. In essence, *NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.*" (emphasis added)[3]

This vital information flow between sensors, decision-makers and shooters in NCW will be carried on a series of "grids," which include the information grid, sensor grids and engagement grids.

> "The information grid provides the infrastructure...for Computing and Communications...[it] provides the means to receive, process, transport, store and protect information for the Joint force. Sensor grids are composed of air, sea, ground, space, and cyberspace based sensors...[to] provide the Joint force with a high degree of awareness of friendly forces, enemy forces, and the environment across the joint battlespace. Engagement grids...enable the Joint Warfighter to employ the speed of command and achieve overwhelming effect at precise places and time[s].[4]

Operation ALLIED FORCE will be examined against this NCW framework, initially with respect to the operational level connectivity provided to U.S. forces in the European theater.

Bosnia Command and Control Augmentation

At the onset of Operation ALLIED FORCE, the Bosnia Command and Control Augmentation (BC2A) system was already in place, serving as a data backbone for real-time video surveillance of the Balkans. Originally deployed in 1996 as a commercial off-the-shelf (COTS) advanced concept technology demonstration in support of the Dayton Peace Accords and Operation Joint Endeavor, BC2A enabled selected locations and commands in Europe to receive a wide-band satellite feed from the Joint Broadcast System (JBS)[5]. The JBS distributed information ranging from CNN to intelligence broadcasts, but most notably downlinked Predator Unmanned Aerial Vehicle (UAV) video. Prior to BC2A employment, this real time, full motion video feed was only available to local commanders in the field, as it was restricted to relatively short line-of-sight ranges limited by geography.

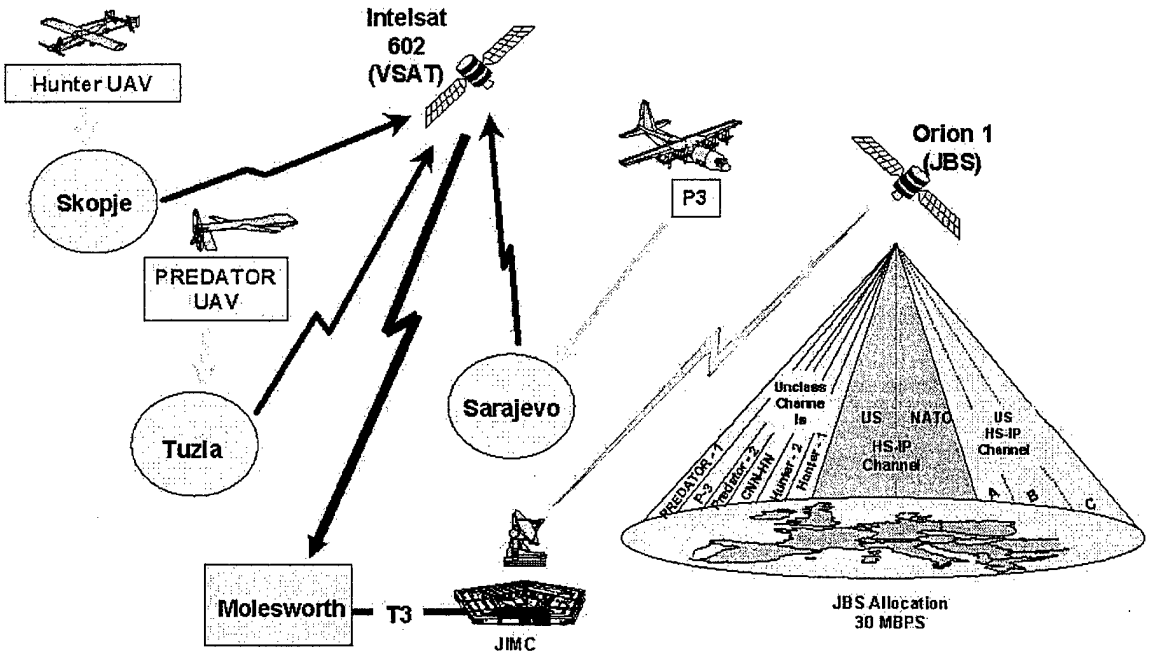


Figure 1. Bosnia Command and Control Architecture (BC2A)[6]

As depicted in Figure 1, BC2A in support of Operation ALLIED FORCE uplinked data streams from Skopje in Macedonia, and both Tuzla and Sarajevo in Bosnia-Herzegovina[†] to a commercial INTELSAT 602 satellite, which then transmitted the data to a ground station situated in Molesworth, United Kingdom. From Molesworth the data was passed via transoceanic link to the Pentagon's Joint Information Management Center (JIMC), which would then rebroadcast the data signal to the commercial JBS satellite positioned over Europe to provide a near real-time broadcast of Balkans-originated information to selected commands. It had been used for the three years prior to Operation ALLIED FORCE as a primary means of distributing Intelligence, Surveillance and Reconnaissance (ISR) video coverage to users throughout Europe.

Video Surveillance

The Predator Unmanned Aerial Vehicle (UAV) was a main source of ISR information, along with electro-optical (EO) capable P-3's. Both aircraft were equipped with a real-time, full-motion video ground surveillance capability, which had proved invaluable to commanders throughout the AOR in monitoring compliance of the Dayton Peace Accords. The advantage with both platforms was their relatively long overhead dwell time, which permitted targets of interest to be surveyed over time, thereby enabling a more complete intelligence picture to be constructed. The BC2A enabled real-time video of ground events to be seen at ground stations ranging from CINCUSNAVEUR in London to Multinational Division headquarters in Bosnia, thereby providing commanders with live video coverage of Stabilization Force (SFOR) operations on the ground in Bosnia. Through the months

[†] See Appendix A for Balkans region map

preceding Operation ALLIED FORCE, BC2A was heavily relied upon, most notably starting in October 1998 in support of the Organization for Security and Cooperation in Europe (OSCE) Kosovo Verification Mission (KVM)[7]. Several KVM teams were inserted into Kosovo following Slobodan Milosevic's agreement to sharply reduce his forces, refrain from repression, and begin negotiations towards an autonomous regime for the province. The concurrent NATO Air Verification Mission was initiated over Kosovo to monitor the unarmed teams, and in order to comply with the agreement's prohibition of manned surveillance platforms, Predator was pressed into service to facilitate unobtrusive team monitoring. Bosnia Command and Control Augmentation provided the means to route the live video to remotely located theater and operational commanders charged with oversight of the mission.

With the availability of live, on-scene coverage, it was quickly realized at EUCOM headquarters that an insatiable desire for Predator video by commanders in the Joint Broadcast System downlink footprint had been spawned. In some headquarters locations it became clear that there was more a *desire* to have the video feed than a true *need*, as Predator video would be displayed on monitors with no concurrent audio to provide context—not unlike having the nightly news on with no sound. Conversely, commanders who did monitor the real-time window on remote operations could find themselves unable to avoid the temptation to influence its mission profile.

When Operation ALLIED FORCE began in late March 1999, Hunter UAV's joined the Predators to provide extensive surveillance and reconnaissance in much the same way as had been seen earlier in Bosnia. The ability of Predator and Hunter to loiter over hostile territory and provide long dwell, full motion video coverage without placing aircrews at risk

underscored the utility of UAV's in combat operations.[8] In addition to using UAV's in these traditional roles, innovative employment tactics were developed whereby they helped locate and target Serbian military forces in Kosovo. By providing target-location data back to NATO's Combined Air Operations Center in Vicenza, Italy, the UAV's helped cue fighter attacks against Serbian forces in the field. When employed in this way, UAV's were used as a component of the forward-air-control system.[9]

The NCW connectivity afforded by BC2A was substantial, and in his assessment of the Kosovo After Action Report, Secretary Cohen noted the importance of BC2A's contribution: "One of the most useful communications capabilities was provided by the wide-band dissemination system, an advanced concept technology demonstration used extensively throughout the conflict for rapidly transmitting high-priority imagery of emerging targets."[10]

Reachback Technology

Operation ALLIED FORCE saw the first extensive use of "reachback" technology for intelligence support, thereby demonstrating the distributed information analysis aspect of NCW. Reachback involved ISR sensor platforms operating over Kosovo while the real-time reduction and analysis of the collected data occurred out of theater.[11] The reachback architecture was analogous to BC2A's, wherein the data stream traveled in a circuitous route from the Balkans, across transatlantic and continental U.S. (CONUS) links. Upon the data stream's arrival on the West Coast, one portion was electronically stripped off and sent back to the *East* Coast for independent analysis, with both parts ultimately returning to the European theater. The trip to either coast took only seconds, enabling time critical

intelligence to be returned to Operation ALLIED FORCE units in minutes. Reachback not only permitted rapid turnaround of crucial information, but substantially reduced the number of intelligence analysts required in Europe, thereby enabling their CONUS-based expertise to be tapped by other theater commanders.

Video Teleconferences

One of the most visible examples of NCW in Operation ALLIED FORCE was the extensive use of video teleconferences (VTC's), held on a daily basis to review progress of operations, coordinate future operations and promulgate further intentions[12]. Key players, , including General Clark, Admiral Ellis, Lieutenant General Short, Vice Admiral Murphy and other subordinate commanders and staff officers regularly attended these conferences[†]. VTC participants spanned the strategic, operational and tactical levels of command, thus greatly compressing normal command-and-control processes.

The ability of high-level commanders to come together by VTC influence tactical operations directly had positive as well as challenging aspects. Among the positive developments was the speed with which commanders and key staff officers could perform essential coordination. One of the challenges was timely documentation and promulgation of the most essential substance of the proceedings, such as the commanders intentions, to those key personnel who did not attend the VTC's. Even for those who did attend, the lack of written documentation often left the participants to question what the commanders intentions really were, which a hard copy message or letter would have served to clarify.

[†] The senior U.S. officers named here occupied NATO billets for Operation ALLIED FORCE (to facilitate U.S. leadership of U.S troops engaged in NATO operations) as well as U.S. Joint Task Force billets for Operation NOBLE ANVIL (the U.S. effort in ALLIED FORCE). These parallel command relationships are graphically depicted in Appendix B.

SIPRNET Connectivity

At HQ USEUCOM, daily routine Secret Internet Protocol Network (SIPRNET) traffic included both classified and unclassified message traffic, point papers, Microsoft Word documents, Microsoft PowerPoint briefs, and seemingly endless e-mails. In March 1997, the Headquarters staff was forwarding virtually all staff action packages destined for General Officer consumption in hard copy form, with drafts of the document for which approval was sought accompanied by all applicable references, printed out and filed under appropriate tabs. Following this very laborious and time consuming effort, the assembled package then passed into the "chop chain" with subsequent approval (or disapproval) passed to the staff action author days, and in some cases weeks, later. This procedure continued for virtually all staff action packages until Operation ALLIED FORCE kicked off in March 1999, when a stark change occurred. Due to the sheer volume of both staff generated paperwork and externally generated information, electronic package submission was initiated, representing a giant leap forward in NCW connectivity on the staff. As virtually all EUCOM Operations Directorate personnel had SIPRNET local area network (LAN) personal computers on their desk, this was an almost universally welcomed change. This represented an "unshackling" of packages from hard copy to electronic form, which were substantially easier to create, pass via e-mail and maintain visibility on. At each higher link in the chain, subordinates would normally be "carbon copied" or "CC'ed" by e-mail, gaining invaluable visibility into what seniors' comments were being appended to the package. In turn, this permitted future packages to be pre-scrubbed to comply with seniors' desires and intentions, both in content or format. This simple increase of NCW connectivity greatly increased

productivity at the theater CINC staff level, with tangible benefits felt in the collaborative planning arena as well.

Unintended Consequences of NCW during ALLIED FORCE

Despite the success of NCW during the Kosovo conflict, the positive side of NCW connectivity tended to obscure some unintended consequences, which, if not properly addressed, could spell trouble in NATO's future. These unintended consequences included a lack of NATO alliance information interoperability as well as U.S. senior leadership involvement in tactical level decisions.

Information Interoperability

One of the most vexing problems during Operation ALLIED FORCE was the lack of information interoperability during NATO combined operations. These problems were manifested in how information was distributed via the supporting C4 infrastructure, as well as how it could be distributed securely regarding the releasability of different classification levels. Dissemination networking and procedures were ad hoc, preventing a common operational picture from being presented to joint and allied commanders.[13] Interoperability between U.S. and NATO data networks was hamstrung due to the lack of a single, integrated data network; and existing networks were inadequate to support the desired tactical, operational and theater-level data among vital NATO information grid nodes.[14] As an illustration, on the U.S. side, HQ USEUCOM and its' service components were exchanging information via SIPRNET at the SECRET level, whereas the closest NATO equivalent system was the Linked Operational Center Europe (LOCE) system, working at the NATO

SECRET level. Classified data sharing rules prohibited introducing NATO SECRET files onto "U.S." SECRET systems, but SECRET information deemed "releasable to NATO" (REL NATO) was acceptable. These restrictions confounded both U.S. and NATO information operations planners, with resultant suggestions made to classify imagery intelligence (IMINT) and signals intelligence (SIGINT) data as SECRET REL NATO, with sources and collection methods protected as needed. This would have afforded wider legitimate data sharing, versus regarding all IMINT and SIGINT products as SECRET with very little REL NATO access.[15]

The Transatlantic Gap

> "Imbalances are growing within the Alliance, between those countries that are investing more quickly in new technologies and capabilities, and those that are proceeding at a slower pace. This is increasingly posing challenges to interoperability, as some Allies move to higher-tech command, control, communications and intelligence equipment.... So we need to ensure that we take advantage of technology to enhance our teamwork, rather than letting technology get between us."[16]
>
> - Lord Robertson, NATO Secretary General

Up through Operation ALLIED FORCE, U.S. forces' far more extensive use of information technology than Europe's forces created a "transatlantic gap" in NATO's warfighting capabilities.[17] The immediate implication was that of European militaries soon being unable to operate alongside the Americans due to European "technological backwardness."[18] Additionally, the concern was that this gap would create tension within NATO, if the U.S. provided the high-tech logistics, lift, intelligence and airpower only it is capable of providing, while European nations found themselves shouldering increasingly dangerous, manpower intensive tasks that could lead to significant casualties.[19] NATO

Secretary General Lord Robertson recently referred to this politically unsustainable situation as "...a two-class NATO, with a precision class and a bleeding class."[20]

Initially adopted in Brussels in 1994 and reconfirmed in Berlin in 1996, the European Security and Defense Identity (ESDI) was envisioned as a means to strengthen the European component of NATO by enabling European allies to take greater responsibility for their common security and defense. While successful operations in Bosnia and Kosovo were not adversely impacted by this divergence in capabilities, many experts argue that European militaries could provide little help in a more challenging engagement.[21] Following Kosovo, European leaders reaffirmed their commitment to the development of the ESDI by nominating NATO Secretary General Javier Solana to the newly established position of High Representative for the European Union's Common Foreign and Security Policy. This was coupled with the decision to merge the Western European Union with the European Union (EU) by the end of 2000, and to create a rapid reaction corps of 50,000 to 60,000 troops under direct EU control by 2003. In spite of these steps towards a more autonomous European self-defense capability, most analysts and policy makers agree that a stronger ESDI will depend less on force structure changes and more on modernization to meet the demands of this new international security environment. In other words, ESDI is seen as a hollow concept without tying it to increased capabilities, which ultimately translates to increased defense spending changes in priorities.[22]

The Defense Capabilities Initiative

To address this imbalance, NATO adopted the Defense Capabilities Initiative (DCI) in April 1999 during NATO's 50th Anniversary Summit in Washington, D.C whilst NATO forces

were fully engaged in ALLIED FORCE operations. As one of the most significant outcomes of the summit, the DCI is intended to enhance allied military capabilities in five key areas: deployability and mobility, sustainability and logistics, effective engagement, survivability of forces and infrastructure, and C2 and information systems.[23] Complicating the DCI implementation issue is the potential for the military criteria for countries vying for NATO admission to be raised to a unattainably high level. When Poland, Hungary and the Czech Republic were admitted to NATO, all were required "to carry out the commitments made prior to accession to increase their defense budgets so that they meet the agreed minimum military requirements."[24] With defense budgets a perennial topic for intense discussion and dissension, it remains to be seen how successful DCI ultimately will be in resolving this technological imbalance, but it's success is seen as crucial for the alliance to remain viable.

Decision Making

Numerous times through Operation NOBLE ANVIL, General Clark as CINCEUR exceeded his theater commander role with regards to real-time Intelligence Surveillance and Reconnaissance (ISR) video coverage and target selection. Several times during Predator missions over Kosovo, General Clark personally redirected the UAV's placement to better facilitate his being able to obtain a view of suspected activity at specific road intersections. The potential for confusion was enormous, as there was little regard for what targets Predator may have been prosecuting at the time. The key in this instance was that although Predator was being flown in support of theater level intelligence it was being operated tactically. Just because General Clark was *able* to redirect it as the operational commander doesn't mean he *should* have.

Historically, delegation of command authority and responsibility to junior subordinates originated as a direct result of geographically separated commanders' inability to communicate.[25] Now, the increasingly available nature of information in an NCW environment carries with it a need for self-discipline on the part of senior commanders, since the "common operating picture" sought through NCW envisions all players at all levels working off the same mental model.[26] The specter of operational commanders meddling in tactical decision making portends insidious long-term consequences. When data is simultaneously available to all command echelons, absolute decisions by senior leaders based on this information will deprive them of the judgment of subordinate intermediate leaders.[27] For example, without an intermediate level to prioritize limited assets or supplies, one can imagine the mayhem that would likely result amongst competing NCW empowered tactical units if adequate, robust self-synchronization controls were not instituted. More importantly though, is the question of how the military will train NCW competent senior leaders in the future if subordinates are trained to expect and rely on uninterrupted direction from above.[28]

Paradoxically, seniors' involvement in lower echelon decisions may be too hard to ignore, as "future knowledge empowered commanders are likely to find it ethically unacceptable to absolve themselves of accountability for lower-level actions of which they have full knowledge and control, and for which they are ultimately responsible".[29] In this age of both zero defects and widespread information availability, there appears to be little room for lapses in judgment in an NCW environment, especially when the preponderance of information will be known by or expected to have been available to commanders at all levels.

Conclusions

During Operation ALLIED FORCE, advances in NCW contributed to the successful execution of a highly coordinated and complex operation, with this increased connectivity evident in several U.S. endeavors. Theater access to real-time, full motion video surveillance of targets of interest permitted operational level decision-makers a view of what had previously been available only to commanders in the field. This capability afforded by the BC2A provided senior leaders a clearer picture of events as they unfolded on the ground in Kosovo, and with it, the ability to make more informed decisions and to provide clearer assessments to their strategic level superiors.

The reliance on reachback technology provided a powerful tool to the European theater intelligence community, leveraging CONUS-based analysts' talents without the expense of maintaining those personnel in theater. Daily reliance on VTC's to facilitate essential warfighting coordination permitted virtual face-to-face contact between senior leaders, providing for subordinates in attendance otherwise unobtainable insights into a myriad of decision-making processes. Finally, SIPRNET data sharing advances at HQ USEUCOM broke the mold of crucial, but arduous staff action package processing, with electronic connectivity greatly enhancing efficiency and productivity. These advances all contributed to increased clarity at the operational commander level, which ultimately assisted in successful prosecution of Operation ALLIED FORCE.

Despite these successes though, NCW in Kosovo was not a panacea for warfighting connectivity in the NATO Alliance setting, as realized upon examination of some unintended consequences in the Kosovo conflict. A major stumbling block was realized in the lack of U.S. and European information interoperability, where communications were hamstrung by

both equipment incompatibilities and classification or releasability mismatches. Additionally, due to the allure of increased wideband video connectivity, U.S. senior operational level leadership at times overstepped its bounds and influenced decisions that should have been left to the tactical level. The solution for intrusive decision making by senior leaders—if there even truly is a *solution* per se—lies with leaders exercising the self-discipline to trust their subordinate commanders while suppressing the tantalizing urge to chase theater or operational "omniscience".

While some in NATO contend that successful ESDI and DCI implementation will solve coalition information connectivity issues, it remains to be seen if our European allies are willing to make the commitment. Their challenge will be to not only commit the precious defense funds needed and appropriately prioritize those funds, but also to cooperate sufficiently as an alliance to keep up with U.S. advances in NCW capabilities. If the commitment is not met, these unintended consequences will likely marginalize anticipated advances in information superiority in the European theater, especially in NATO alliance military operations.

> "Whether or not the Defence [sic] Capabilities Initiative will succeed is as yet an open question. But one thing is certain: If it does not ultimately translate into concrete improvements in the European component of NATO's force posture, the long-term viability of the transatlantic link will come under growing pressure from a U.S. Congress increasingly skeptical about Europe's commitment to keeping pace with the Revolution in Military Affairs."[30]
>
> - Dr. Elinor Sloan
> Directorate of Strategic Analysis
> National Defence Headquarters, Canada

Endnotes

[1] Sun Tzu, "The Art of War"; trans. Samuel B. Griffith, New York: Oxford University Press, 1971, p. 65

[2] Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 29.

[3] David S. Alberts, John J. Garstka and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, (Washington: DoD C4ISR Cooperative Research Program, 1999), 2.

[4] Joint Chiefs of Staff, "Information Paper: Observations on the Emergence of Network Centric Warfare," http://www.dtic.mil/jcs/j6/education/warfare.html, 4 May 2000.

[5] _____, "How BC2A Came Together," Bosnia Command and Control Augmentation--Leader's Leader's Overview, January 1998, <http://www.disa.mil/d3/bc2a/briefings/leaders//leader03.html>.(4 May 2000)

[6] Pamela O. Howard, "BC2A Video Architecture," Bosnia Command and Control Augmentation (BC2A) VSAT Transition, 14 September 1999, <http://www.eucom.mil.events/gbs/aar/bc2axsep99.ppt> (6 May 2000), 38

[7] Department of Defense, Kosovo/Operation Allied Force After-Action Report (Washington: 1999), 2

[8] William S. Cohen and General Henry H. Shelton, "Joint Statement On The Kosovo After Action Review" DefenseLINK News, <http://www.defenselink.mil/news/Oct1999/b10141999_bt478-99.html>, 14 October 1999.

[9] DOD, Allied Force AAR., 57

[10] Cohen and Shelton "Joint Statement"

[11] DOD, Allied Force AAR., 55

[12] Ibid., 28

[13] DOD, Allied Force AAR., 49

[14] Ibid.

[15] Ibid.

[16] Lord Robertson, "Rebalancing NATO for a Strong Future," Defense Week Conference, Brussels, 31 January 2000, < http://www.nato.int/docu/speech/2000/s000131a.htm>, 7 May 2000

[17] David C. Gompert, Richard L. Kugler and Martin C. Libicki, Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs, (Washington: National Defense University Press, 1999), 4.

[18] Dr. Elinor Sloan, "DCI: Responding to the U.S.-led Revolution in Military Affairs," NATO Review, 25 April 2000, <http://www.nato.int/docu/review/2000/0001-02.htm>, 7 May 2000

[19] Ibid.

[20] Robertson, "Rebalancing NATO"

[21] Sloan, "DCI"

[22] Ibid.

[23] Cohen and Shelton "Joint Statement"

[24] General Wesley K. Clark, "Statement before the Senate Armed Servces Committee," 29 February 2000, <http://www.eucom.mil/

[25] James R. FitzSimonds, "The Cultural Challenge of Information Technology," Naval War College Review, Summer 1998, <http://www.nwc.navy.mil/press/Review/1998/summer/art1su98.htm>, 3 May 2000,

[26] Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," U.S. Naval Institute Proceedings, January 1999, <http://www.usni.org/Proceedings/Articles99/PRObarnett.htm>, 3 May 2000.

[27] Donald E. Walker, ed., Information System Science and Technology (Washington: Thompson Book Company, 1967), 106.

[28] FitzSimonds, "Cultural Challenge"

[29] Ibid.

[30] Sloan, "DCI"

Bibliography

_____. "How BC2A Came Together." Bosnia Command and Control Augmentation--Leader's Leader's Overview. January 1998. http://www.disa.mil/d3/bc2a/-briefings/leaders//leader03.html.

Alberts, David S., Garstka, John J. and Stein, Frederick P. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington: DoD C4ISR Cooperative Research Program. 1999.

Barnett, Thomas P.M. "The Seven Deadly Sins of Network-Centric Warfare." U.S. Naval Institute Proceedings, January 1999.

Cebrowski, Arthur K. and Garstka, John J. "Network-Centric Warfare: Its Origin and Future." U.S. Naval Institute Proceedings, January 1998.

Clark, Wesley K. "Statement before the Senate Armed Services Committee," 29 February 2000, < http://www.eucom.mil/posture/2000/2000_posture_statement.htm>.

Cohen, William S. and Shelton, Henry H. "Joint Statement On The Kosovo After Action Review" DefenseLINK News. 14 October 1999<http://www.defenselink.mil/ news/ b10141999-_bt478-99.html>.

DiNardo, R.L. and Hughes, Daniel J. "Some Cautionary Thoughts on Information Warfare." Airpower Journal, Winter 1995.

FitzSimonds, James R. "The Cultural Challenge of Information Technology." Naval War College Review, Summer 1998.

Gompert, David C., Kugler, Richard L. and Libicki, Martin C. Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs. Washington: National Defense University Press. 1999.

Howard, Pamela O. "BC2A Video Architecture," Bosnia Command and Control Augmentation (BC2A) VSAT Transition, 14 September 1999, <http://www.eucom.mil.events/gbs/aar/bc2axsep99.ppt>.

O'Hanlon, Michael. Technological Change and the Future of Warfare. Washington: Brookings Institution Press, 2000.

Robertson, Lord. "Rebalancing NATO for a Strong Future." Defense Week Conference. Brussels. 31January 2000. < http://www.nato.int/docu/speech/2000/s000131a-.htm>.

Sloan, Elinor. "DCI: Responding to the U.S.-led Revolution in Military Affairs." NATO Review. 25 April 2000. <http://www.nato.int/docu/review/2000/0001- 02.htm>.

Tzu, Sun. "The Art of War". trans. Samuel B. Griffith. New York: Oxford University Press. 1971.

U.S. Department of Defense. Kosovo/Operation Allied Force After-Action Report. Washington: 1999.

U.S. Joint Chiefs of Staff. "Information Paper: Observations on the Emergence of Network Centric Warfare." <http://www.dtic.mil/jcs/j6/education/warfare.html>.

_____. Joint Doctrine for Command and Control Warfare (Joint Pub 3-13.1) Washington, D.C.: 9 October 1998.

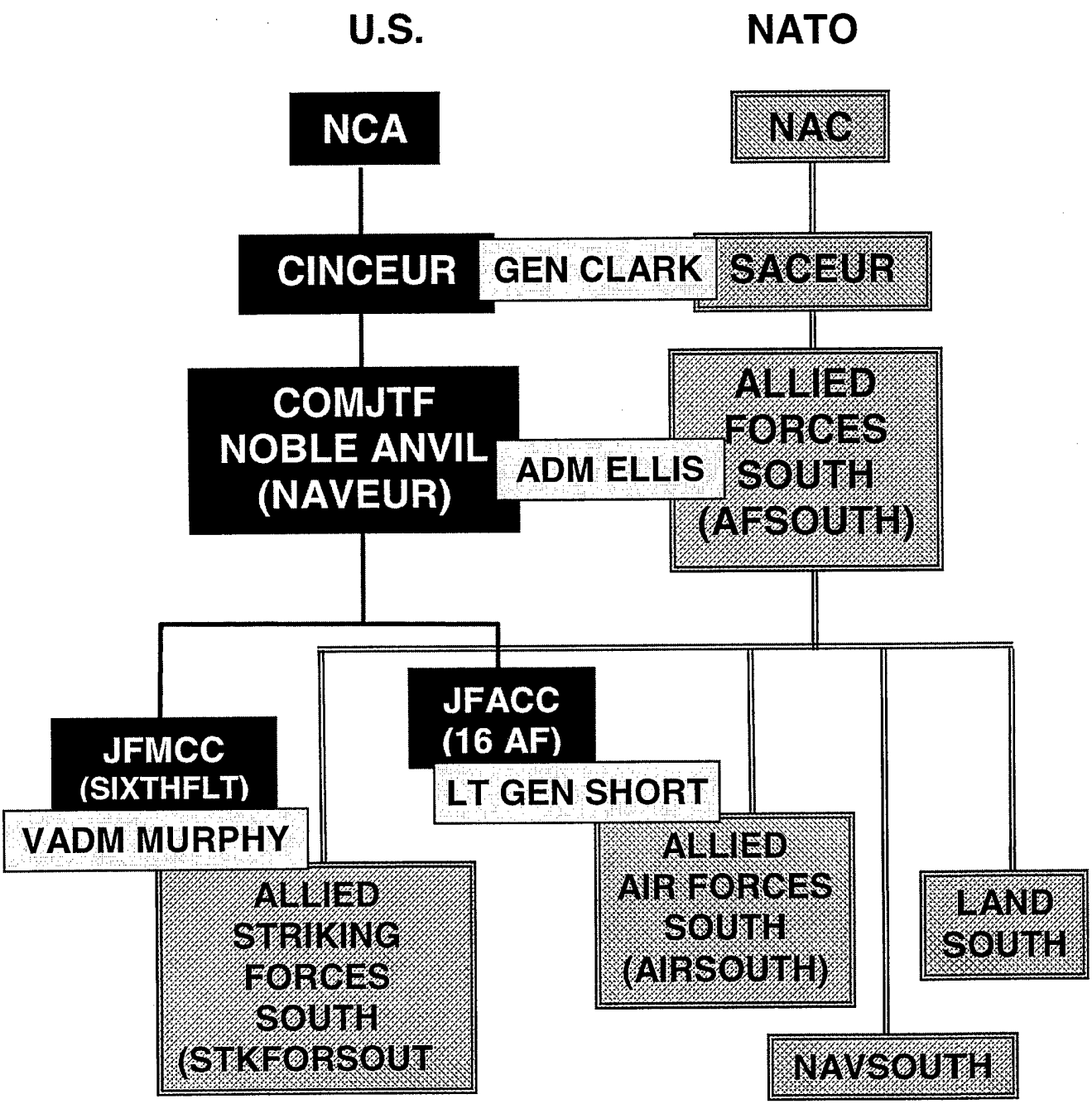
_____. "Joint Vision 2010" Joint Electronic Library CD-ROM Washington, D.C.: Joint Chiefs of Staff. August 1999.

Walker, Donald E. ed. Information System Science and Technology. Washington: Thompson Book Company, 1967.

Appendix A

The Balkans Region

Appendix B



Primary Dual Hatted U.S. - NATO Billets
ISO Operation ALLIED FORCE/ Operation NOBLE ANVIL