NAVAL WAR COLLEGE
Newport, R.I.

IS THERE A PLACE FOR OPERATIONAL DECEPTION IN THE AGE OF INFORMATION WARFARE?

by

Richard M. Schmitz
LtCol USMC

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: _____

5 February 2001

Advisor: CDR Mike Michaels USN

_____

Moderators: Professor Elizabeth McIntyre
CAPT Patrick Toohey USN

#15

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority: N/A

3. Declassification/Downgrading Schedule: N/A

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):
IS THERE A PLACE FOR OPERATIONAL DECEPTION IN THE AGE OF INFORMATION WARFARE? (U)

9. Personal Authors: LtCol Richard M. Schmitz USMC

10. Type of Report: FINAL

11. Date of Report: 5 February 2001

12. Page Count: 24

12A Paper Advisor (if any): CDR Mike Michaels USN

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: OPERATIONAL DECEPTION, INFORMATION WARFARE, INFORMATON OPERATIONS, MILITARY DECEPTION, NETWORK CENTRIC WARFARE

15. Abstract: One of the principle tenets of Operational Art concerns Operational Deception as a tool for the Commander to use in affecting success on the battlefield. The age of information warfare, as a new concept linking networks toward more effective war fighting and denying one's adversary the capability to do the same, must still encompass the Operational Art of War tenets. Embracing the concepts of information warfare without adequately planning for Operational Deception, shortchanges the Commander in his ability to utilize all of his capabilities to defeat his adversary. Operational Deception still plays a critical role as a force multiplier and continues to contribute to military and political victory.

Information operations and information assurance with regard to information warfare deal with denying an adversary access to our networks and the critical information that flows across these links. Operational Deception calls for misleading an adversary by deceiving him with false or ambiguous information and causing him to act in a way that is to our advantage. By denying him access to our networks and "locking out" his ability to use his networks, the Operational Commander causes a dilemma in not being able to effectively utilize Operational Deception. The paradox concerns providing a means for the enemy to receive the deceptive information and our ability to monitor him for effective evaluation of the deception's success. Despite the challenges, a Commander would be remiss not to plan for and execute Operational Deception to gain victory in the age of information warfare.

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: C

Security Classification of This Page Unclassified

Abstract of

IS THERE A PLACE FOR OPERATIONAL DECEPTION
IN THE AGE OF INFORMATION WARFARE?

One of the principle tenets of Operational Art concerns Operational Deception as a tool for the Commander to use in affecting success on the battlefield. The age of information warfare, as a new concept linking networks toward more effective war fighting and denying one's adversary the capability to do the same, must still encompass the Operational Art of War tenets. Embracing the concepts of information warfare without adequately planning for Operational Deception, shortchanges the Commander in his ability to utilize all of his capabilities to defeat his adversary. Operational Deception still plays a critical role as a force multiplier and continues to contribute to military and political victory.

Information operations and information assurance with regard to information warfare deal with denying an adversary access to our networks and the critical information that flows across these links. Operational Deception calls for misleading an adversary by deceiving him with false or ambiguous information and causing him to act in a way that is to our advantage. By denying him access to our networks and "locking out" his ability to use his networks, the Operational Commander causes a dilemma in not being able to effectively utilize Operational Deception. The paradox concerns providing a means for the enemy to receive the deceptive information and our ability to monitor him for effective evaluation of the deception's success. Despite the challenges, a Commander would be remiss not to plan for and execute Operational Deception to gain victory in the age of information warfare.

Table of Contents

INTRODUCTION

Sun Tzu's quote that; "All warfare is based on deception"[1] is still relevant in today's age of high-speed information networks and near real time intelligence analysis. These means are utilized by the Operational Commander to increase his ability to make faster decisions on the battlefield to outwit his enemy and bring about decisive victory. With the dawn of the 21st century and the ongoing information technology revolution in military affairs, US Military Strategy has highlighted the visionary change of information superiority as a key enabler in the transformation of a Joint Force Commander's operational capabilities and the evolution of command and control.[2] Information superiority leads to superior knowledge and, therefore, to decision superiority, or the ability to make better decisions faster than an adversary.[3]

Although this statement sounds simple enough, fog and friction in battle are still prevalent. To overcome this age-old challenge, information operations were developed to prevent an enemy from gaining information superiority while protecting one's own information gathering capability. Thus we have entered an age of information warfare. Within this new concept, the target of information operations and deception remains the decision maker.[4]

The age of information warfare, as a new concept geared toward more effective war fighting and denying one's adversary the capability to do the same, transcends all levels of war to include the Operational level. Operational Deception, as a tool for the Commander, aids in achieving surprise, and indirectly security and economy of effort. Embracing the concept of information warfare without adequately planning for Operational Deception, short changes the Commander in using all of his capabilities to defeat his adversary. *Operational Deception still plays a critical role as a force multiplier in the age of information warfare and continues to contribute to military and political victory in the 21st century.*

Information operations and information assurance, with regard to the relatively new concept of information warfare, deal with denying an adversary access to our networks and the critical information that flows across these links. Operational Deception as a component of information warfare calls for misleading an adversary by deceiving him with false or ambiguous information and causing him to act in a way that is to our advantage. By denying him access to our networks and "locking out" his ability to use his networks, the Operational Commander causes a potential dilemma in not being able to completely utilize Operational Deception. The paradox concerns providing a means for the enemy to receive the deceptive information and our ability to monitor him for effective evaluation of the deception's success. Despite these challenges, a Commander would be remiss not to plan for and execute Operational Deception to gain leverage in the new age of information warfare.

I will address the issue of the utility of planning for and executing Operational Deception in the age of information warfare by first framing the concepts and terminology to allow for a common understanding of the thesis presented in this paper. I will highlight how an adversary can use deception to his advantage against the US Operational Commander. Through examining the most recent case study of Operation Allied Force (Kosovo Air Offensive) I will identify opportunities taken and missed by the United States military with regard to Operational Deception against the Serbs. Furthermore, I will make recommendations for a CINC toward the use of military deception in the age of information warfare and will draw conclusions to fortify my original thesis that Operational Deception still plays a critical role as a force multiplier and continues to contribute to military and political success in the age of information warfare.

BACKGROUND: KEY DEFINITIONS

In order to grasp the change in the nature of war due to the refinement of information technology, one must first agree on a common set of parameters. This understanding becomes critical to reaching the conclusion that Operational Deception plays a crucial role in information warfare for the Commander. First we must define deception, then military deception and, specifically, Operational Deception and how it relates to information warfare. Part of conceptualizing information warfare is to define information operations and the dual role it plays in aiding the Joint Commander to achieve battlefield success. As we will see, information operations can be both offensive and defensive. Deception falls under the realm of offensive information operations. Lastly, we will touch on the six steps of the military deception planning process as spelled out in the Joint Doctrine for Military Deception Pub.

Deception is seen as those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.[5] **Military Deception** is seen as the actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. There are six principles of military deception: focus, objective, centralized control, security, timeliness and integration.[6] There are also five categories of military deception, one of which is Operational Military Deception.[7] **Operational Military Deception** is military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is

planned and conducted in a theater of war to support campaigns and major operations.[8] Deception planning should occur simultaneously with operation planning and is targeted at the enemy decision maker, not normally the enemy's intelligence system.[9] In addition, deception operations will not intentionally target or mislead the US public, Congress or the US news media. Misinforming the media to influence US decision makers and the public is contrary to current DOD policy.[10] Yet, deception plays a critical role in information warfare.

Information Warfare (IW) is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[11] IW primarily concerns gathering information, processing it, and manipulating it for both offensive and defensive purposes.[12] **Information Operations (IO)** are actions taken to affect adversary information and information systems while defending one's own information and information systems. Information operations can be either offensive or defensive.[13] **Offensive Information Operations** is the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, *military deception,* psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack.[14]

The Joint Doctrine for Information Operations further states that military deception requires a thorough knowledge of an opponent, his decision making process and places attention on how the Joint Force Commander would like the enemy to *act* at critical points in the battle. Military deception operations depend on intelligence operations (and planners) to identify appropriate targets, assist in developing a credible deception story and assess the

effectiveness of the military deception plan. It is a top-down planning process.[15] A key factor in deception planning involves cost and risk. A Commander has to be willing to allocate resources and personnel to planning and executing a deception plan and understand the risk involved to the success of the overall operation if the deception plan fails.[16]

Concurrent with the operational planning process, the six-step deception planning process should ensue. As part of the overall mission analysis, **deception mission analysis** should take place. The JFC considers how deception can support mission accomplishment. In step two, the JFC gives his **deception planning guidance** stating the deception objective for the operation. Next, the **staff deception estimate** is conducted as part of the operation estimate. The deception planners gather and analyze adversary information to try to determine enemy decision makers and their preconceptions and any enemy courses of action (COAs) they are likely to take. The planners develop deception COAs in support of the friendly operation COAs. In step four; the **Commander's deception estimate** results in the JFC selecting a supporting deception COA to the actual operation COA. The deception planners must work closely with the operation planners to ensure that the deception COA mutually supports the operation COA. The deception COA matures into a complete **deception plan or order development** in step five. This is the most time consuming phase and results in five actions: completing the story, identifying the means, developing the event schedule, identifying feedback channels and developing the termination concept. Again, time is the most crucial factor in this phase to ensure that the deception can effectively make the enemy decision maker act to one's advantage on the battlefield. The final step involves **deception plan/order review and approval** by the JFC. Only a limited number of personnel should be privy to the deception plan review and approval. After approval, execution commences.[17]

KOSOVO: A CASE STUDY

The first case study involving information warfare and operational deception took place in Operation Allied Force in support of air operations above Kosovo and Serbia. The 78-day air offensive waged against Serbia involved strikes originating from 22 different air bases in seven countries without suffering a single combat fatality.[18] The US-led NATO Operation was an example of an asymmetric conflict. Serbian President Slobodan Milosevic, from the perceived position of weakness, still had the ability to effectively utilize his deception assets in the information war against the United States and its Allies.[19] A unique aspect of the armed conflict was the absence of interjecting Allied ground troops prior to the cessation of hostilities. President Clinton's announcement that, "No ground troops are to be employed in Kosovo," set a new standard for "anti-deception" that certainly hindered the Operational Commander's ability to employ an effective deception plan involving the perceived probability of a ground force invasion.[20]

According to LtCol. Glaze USAF, a staff officer in the JCS Policy and Doctrine Division, the US military's overall IO effort met with limited success during Operation Allied Force.[21] He commented that DOD has yet to conduct a true 21st century IO campaign.[22] He further explained that a new definition of IO was needed that includes hacking into enemy systems to implant false data or communicating misinformation as part of the definition with regard to military deception.[23] The concepts were ill-defined and practical application suffered.

Yet, notable achievements in information technology were introduced by US forces that require protection against counter-deception to include safeguarding web-based technologies for coordination and information sharing, video teleconferencing for C2 and the use of e-mail

for coordination and official tasking.[24] As will be highlighted later in this paper, the combat application of this information technology showcases the ability of the Commander to react faster than his adversary, but also opens up a new potential for deception operations by a willing and capable enemy. However, the use of this capability for friendly deception operations is also now available if properly planned for and executed.

Other aspects of IO that were employed in Kosovo by the JFC included dropping 104,000 propaganda leaflets, conducting 88 electronic warfare missions to broadcast pro-Allied messages, setting up an internet site (www.serbia-info.com) to counter the Serb propaganda[25] that could all have applicability for further exploitation in future deception operations to either mislead or confuse the enemy decision makers to act in ways more advantageous to the US Operational Commander. In addition, C-130 missions were flown to broadcast pro-Allied TV messages to the Serb population as well. Along with leaflet drops, this method of psychological ops met with minimal success due to varying factors like weather and terrain masking.[26] Using these means as a potential way to present a deception story to the Serb enemy leaders was not evidently used. Yet, these methods could be used for dissemination of misinformation as a deception application and are worth pursuing in future conflicts.

Although the enemy decision maker might possibly consider this method of delivery of a deception story as suspect, these deceptive psychological operations still would have a negative effect on the adversary's population by showing how pervasive the US capability is in interfering with the everyday functions of the citizenry. In a related story, US and NATO forces imposed a "gray out" on information supposedly for operational security reasons to the US media who in turn "badly misrepresented the size and scope" of the air offensive in its early days to make it seem like a massive operation was taking place. In an effort to scoop

each other, the media didn't assess the information and events with enough scrutiny to realize that the effort wasn't as big as they perceived. The press accepted the "official line" that the air war was intensifying and then accused the US military of deception and secrecy, which, as stated earlier, is counter to current DOD policy on informing the media.[27] One can see how even *inadvertent* misperception in open sources can also be used for deceptive purposes against the enemy as well.

With the advent of the large-scale use of data information systems by US and NATO forces, the issue of information releasability to coalition partners and the media became a concern. These same types of concerns barred any integration of deception planning between US and NATO IO planners.[28] The higher classification of US gathered information and signals intelligence data has the effect of prohibiting the use of collaborative deception planning and thus negated the use of operational deception as a force multiplier in the successful outcome of the Operation.[29] In addition, to bridge the interoperability gap, some information sharing was done on unsecured links that were susceptible to enemy probing and possible deception interjection.[30] ADM James Ellis USN, Commander of Allied Forces in Southern Europe during Operation Allied Force, commented that, "the enemy was much better at this [media-manipulation efforts and propaganda attempts as part of an information effort] than we were...and far more nimble."[31] As Gen. Gordon Sullivan USA, former Army Chief of Staff, stated, "information is the currency of victory on the battlefield."[32] The opponent who is able to master it to his own advantage, through superior IO to include the use of deception, will benefit in the long run.

Operation Allied Force also saw the first extensive use of sensor platforms forward deployed while the data reduction and analysis components remained at the home stations.[33]

The use of this "reach back" capability reduced the need for a large number of forward deployed analysts and could have had negative results on the screening of enemy deceptive information by a sufficient amount of forward deployed intelligence analysts if the deceptive material had been interjected into the long haul information systems used by these forward deployed operational units. The heavy reliance on large information databases created and maintained in the rear echelons without an effective method of screening the information by frontline analysts for accuracy could have aided astute enemy deception planners in causing forward deployed commanders to assume that this information was ground truth and therefore act in ways advantageous to the Serbs.

As demonstrated by Operation Allied Force, advantages in technology and supposed information superiority did not necessarily translate into a clear-cut victory in the information war against the asymmetric threat posed by Milosevic. In fact, the Journal of Electronic Defense gave the deception effort on its IW Report Card of Operation Allied Force a "failing grade."[34] Col Hugo Valdivia, Chief of the USAF's Defensive Information Warfare Division at Air Force Headquarters, commented that many issues were still being addressed concerning the ability to utilize varying methods of operational deception in IO that specifically involved the legality of the rules of engagement in conducting Operation Allied Force. He speculated that IW was used offensively but couldn't confirm the use although "he was sure there was a plan."[35] It's apparent that the JFC didn't utilize Operational Deception to its fullest IW potential in Operation Allied Force.

However, two of the lessons learned from operations in Kosovo concerned the shortage of perception management expertise[36] and a lack of articulated Commander's guidance, which directly affected IO planning and support.[37] Although the deception terminology was not

specifically stated in the Joint Unified Lessons Learned System (JULLS) examples, one can infer that a lack of guidance in IO planning and the absence of perception management expertise adversely impacted on whatever deception planning did occur. As spelled out in the Joint Pub on Military Deception, the planning process calls for early and definitive guidance by the JFC with regard to formulation and choice of a Deception COA and development of the ensuing Order/Plan for execution in achieving the overall mission. Although Operation Allied Force just recently concluded and the opportunity to publish information on deception in the conflict is still in its infancy (if concerted deception planning and execution even took place), the Kosovo case study leads one to believe that this process and the desired end state of Operational Deception in the Information War against Serbia was not completely adhered to nor succinctly realized in the successful execution of Operation Allied Force.

RECOMMENDATIONS: GUIDANCE FOR THE CINC

With Operation Allied Force's apparent missed opportunity to effectively use Operational Deception to cause the Serbian military and political decision makers to act in ways more advantageous to the Allied effort, one can still draw out lessons and make recommendations for future operations. With a better understanding of the concepts of information warfare and military deception's role in recent conflicts in the age of information warfare, doctrine will be laid out in a more concrete fashion. As a result of the Kosovo experience, improving upon and clarifying doctrine better educates today's military leaders on the feasibility of IO and the part that deception plays in achieving a desired end state. With better-educated leaders,

training and exercises can be conducted focusing and utilizing this understanding as the basis to ensure that deception planning is executed and deception is carried out with a higher degree of success. This success can be gauged as effective if the deception's target audience committed forces or resources in ways that the Operational Commander could exploit or the adversary made decisions that benefited the overall plan in accomplishing the specific Operational objectives. The deception planning process, as highlighted previously in this paper seems well thought out and practical, yet in Operation Allied Force, there seems to be little evidence that the planning process was used or discounted as dysfunctional. It appears that the Kosovo case study bears out that the JFC largely ignored the doctrinal layout of deceptive planning even though it appears to be a sound methodology for effective employment of deception and also counter-deception.

Introspection on US defensive IO capabilities (counter-deception) will help the JFC evaluate his weaknesses and assist in determining enemy deception strengths causing US actions that benefit the enemy. By analyzing US weaknesses, the Operational Commander can implement actions needed to improve on his ability to thwart enemy deception and therefore better use offensive US IO methods, like military deception, to cause the enemy commander to deleteriously act based on his perception management. The focus of deception on this level must also include an analysis of counter-deception to better understand how to employ one's own deception that would cause enemy action which would adversely affect his lines of communication, force disposition, logistics, command and control and related processes to achieve US objectives quicker and at less of a cost. [38]

An example of this introspective process was seen in Exercise Eligible Receiver in 1997 and countering computer network attacks in 1998 during the deployment phase of Operation

Desert Thunder. During Exercise Eligible Receiver, CJCS realized how vulnerable DOD networks were to enemy intrusion and therefore interjection of deceptive tactics and techniques into our information systems. Within days of the exercise's start, NSA hackers had "rendered impotent the PACOM C2 elements and effectively could have shut down the US electrical power grid."[39] Efforts to track the attackers were largely unsuccessful and the hackers breached the Pentagon's unclassified global computer network using Internet service providers and phone connections to virtually conduct covert operations from anywhere.[40]

Access to both classified and unclassified military networks allows an adversary to use these conduits to mislead and confuse the Operational Commander to act in ways that will benefit the enemy's efforts at success on the battlefield. Learning from a position of supposed information superiority against adversaries that are perceived as less than a match against US technology is not only a lesson in humility, but has great merit in using the same techniques to execute a deception plan against an opponent who is even less capable of detecting the deception plan conducted against him. The Operational Commander must first ensure his information systems are capable of withstanding computer network attacks and has sufficient trust that his efforts at counter-deception are adequate to conduct a deception plan with less risk involved in being uncovered by the enemy.

An example of recent defensive IO employment which in turn could support future deception operations involved efforts to curb DOD web sites from "giving away the farm" on critical information. One USAF reserve unit surveyed 800 web sites and found 1,300 "discrepancies" including 10 postings of Pentagon war plans, 20 detailed facility maps such as the alternate Joint Communication Center for US nuclear forces, exercise force lists, frequencies, call signs and Identification Friend or Foe (IFF) data squawks for pilots.[41] The

implications are an enemy can exploit his deceptive methods through simple hacking or browsing. The upside of this discovery is that the Operational Commander can create "honey pots" which use deception to divert hackers away from the classified info and assist in trapping them for use by friendly forces. The newly established Joint Task Force for Computer Network Defense has begun to "tag" hackers' stolen information so that in peacetime, law enforcement agencies can catch and prosecute the criminals.[42] Applications of this technology and methodology could be applied and incorporated as part of a deception plan directed at a target audience. With the growth of the global information grid, even adversaries perceived to be weak have the capability to hack into unclassified and possibly classified data networks.

Not only should the JFC improve his own defensive IO posture through such actions as safeguarding information online, but by collaborating with trusted private industry sectors, greater defensive IO capabilities can ensure that enemy deception does not achieve its intended objectives. At the same time, the JFC should be conducting his own deception via the same type of enemy offensive IO "hacking" and computer network attack/monitoring means. Another example of this effort is seen by high-tech firms setting up their own computer defense hub to share and analyze information about thwarting concerted cyber-threats. Such firms as AT&T, Cisco Systems, IBM, Intel, Microsoft and Computer Sciences Corporation have all joined together in this endeavor.[43] The next step should be entering into a collaborative effort with the US Government and DOD. Even challenges by companies like Argus Systems Group, makers of computer security products, who give away money for attempts to hack into their secure systems[44] has an application in the realm of deceptive planning on the part of the Operational Commander and his staff. Denying the opportunity to

gain access and information from one's own network systems and attempting to exploit the enemy's systems in order to plant deceptive stories and monitor feedback of the target audience directives to his tactical units allows the JFC to more effectively capitalize on his thorough deception planning and execution.

The JFC is responsible for placing the right amount of emphasis on the importance of deception in the deliberate and crisis action planning process. The process, as spelled out in the Joint Pub, appears to be a sound methodology that a JFC must emphasize to his "Deception Planning Cell" and demand that it be applied for the overall benefit of the Operational Plan. At a minimum, the JFC needs to ensure that his "Deception Planning Cell" is comprised of highly qualified personnel from the J2, J3 (should take lead on the planning as the Deception Plan becomes part of Annex C of the Operation Order/Plan), J6, PAO, SJA and other principle staff members as he sees appropriate to ensure that the deception planning process gets the attention it deserves in order to be effective and a force multiplier for the Operational Commander.

The JFC needs to first understand the concepts of information warfare, information operations and the role of deception as a force multiplier in accomplishing the mission. Educating himself and his staff on current doctrine and the still changing DOD IW organizations that deal with information operations and deception and could be called upon by the JFC to assist in his deception planning, ensures that his command is capable of meeting the challenges presented by an adversary while also preparing a deception course of action. The JFC needs to allocate the proper amount of qualified personnel, money and resources to accomplish the task of planning for deception in the age of information warfare and that focused training is devoted to meet this objective.[45] Staff training through seminars,

briefs, command post exercises, war games, and conceptual exercises during the preparatory phases of field exercises or deployments are all examples to improve upon his ability to attain a staff capable of planning and executing deception operations in a conflict.[46]

The routine nature of organizing an ad-hoc Joint Task Force or the come-as-you-are Operational Commander and his staff needs to safeguard against the tendency of ad-hoc deception planning.[47] As the battle for information superiority intensifies, so must the effort by the Operational Commander to ensure that he has the requisite capability to exploit strengths in this area by utilizing the tools available to him. If the Operational Commander does not feel he has adequately prepared for the use of Deception, then he should request augmentation of personnel and resources and assistance from units and agencies that are capable of providing the Offensive IO and deception support required to assist the over-arching Plan. Deception, planned at the Operational level and coordinated with subordinate deception plans, is still a viable means to meet the challenges presented by information warfare and will cost-effectively assist the Commander in mission accomplishment.

CONCLUSIONS

Carl von Clausewitz stated that, "the higher the military rank, the greater is the degree to which activities are governed by the mind, by the intellect, by insight. Consequently, boldness, which is a quality of temperament, will tend to be held in check."[48] Yet, boldness is what is required by a JFC to execute a Deception Plan on the Operational level. Due to the high speed of information flow on the modern battlefield and the quest for certainty, aided by network centric warfare, the time it takes to create and interject a deception story and the

ability to maintain a deception from enemy discovery tends to become problematic and short-lived. The days of planting a ruse over months similar to examples of feigning the landings in World War II, may very well be negated by the shortened decision cycle achieved through IT and network centric warfare of the 21st century. Overcoming a hesitation to act until a preponderance of supporting intelligence, from numerous sources, is received by the JFC still requires boldness to overcome operational paralysis due to information overload. Rather than ignore the deception planning process or pay it little attention while focused on the Operational Plan, a JFC must understand that deception, despite information warfare, is still viable and cost effective requiring him to utilize this tenet of Operational Art to his advantage. Some argue that superior information technology and the use of satellites cancels out the ability to effectively use deception, yet one should not assume that an enemy would not operate by the same perception. On the contrary, the "weaker" opponent may see the use of deception as a great equalizer in his effort to bring about victory.

The US military maintains a distinct advantage in information collection, analysis, speed of decision-making and dissemination of information and directives through the use of IT. From this position of information and decision superiority, the JFC depends heavily on his information systems and sensors. This dependency is beneficial in throwing an adversary off balance by anticipating his moves and staying within his decision-making loop, yet can also be an "Achilles Heel." In attempting to level the playing field, an opponent with limited technological capability can still pose a threat to the Operational Commander through asymmetric cyber-attacks and use of deception in the information war.

The effectiveness of deception depends on the availability of information that a Commander has at his disposal in which an adversary can surreptitiously interject deception

and his penchant to do so.[49] As demonstrated in Kosovo, the plethora of info databases and intelligence available at the stroke of a key was immense and virtually unquestioned as accurate. Therefore, the Operational Commander must not become complacent or overly reliant on the IT-based revolution in military affairs without sufficient analysis of the information and intelligence at his disposal. Similarly, due to the rapid speed of access to information (accurate or deceptive) on the enemy, the JFC needs to ensure that the tenet of Operational Deception is not discounted due to the apparent time it takes to plan and execute military deceptions. The ancient Chinese adage: "There can never be enough deception..." still rings true on the modern battlefield of the 21st century.[50]

The Operational Commander's mission dictates that he uses all means available in the successful pursuit of victory. Information warfare becomes a means to achieve the desired objectives. Both Offensive IO (deception) and Defensive IO (counter-deception) can assist the JFC in obtaining battlefield success. Protecting against the enemy deception and utilizing one's own deception plan to cause the opponent to act in ways that are advantageous to the JFC's overall mission is still as relevant in the age of information warfare as it was in Sun Tzu or Clausewitz' day. Understanding the new concepts of IW and its relationship with Operational Deception and incorporating them into common practice through analyzing lessons learned from past conflicts or future peacetime training, better prepares the leader to meet the challenges of fog and friction in the arena of information warfare. The JFC must not discount the utility of deception as a force multiplier in his quest for military and ultimately political victory in the age of information warfare. Deception still plays a critical role and continues to contribute to Operational-level success in the 21st century.

END NOTES

[1] Sun Tzu, The Art of War, (New York, NY: Oxford University Press, 1971), p. 66.
[2] Chairman of the Joint Chiefs of Staff, Joint Vision 2020 America's Military: Preparing for Tomorrow, (Washington DC: General Printing Office), p. 3.
[3] Ibid., p. 8.
[4] Ibid., p. 29.
[5] Joint Pub 1-02, The DOD Dictionary of Military and Associated Terms, (Washington DC: General Printing Office, 23 March 1994 As Amended through 14 June 2000), p. 124.
[6] Joint Pub 3-58, Joint Doctrine for Military Deception, (Washington DC: General Printing Office, 31 May 1996), p. v.
[7] Joint Pub 1-02, p. 289. The other categories are: Strategic, Tactical, Service, and Military Deception in Support of Operations Security.
[8] Ibid.
[9] Joint Pub 3-58, p. I-3.
[10] Ibid., p. I-4.
[11] Joint Pub 1-02, p. 221.
[12] Nick Cook, "Brain Storming", in Jane's Defense Weekly, 16 August 2000, database on-line. Available from http://homepage.mac.com/ebird1/s20000818/s20000818brain.htm, p. 1.
[13] Joint Pub 1-02, p. 221.
[14] Ibid., p. 329.
[15] Joint Pub 3-13, Joint Doctrine for Information Operations, (Washington DC: General Printing Office, 9 October 1998, p. II 4-5.
[16] Joint Pub 3-58, p. IV-1.
[17] Ibid., p. IV2-8.
[18] Frederic H. Levien, "Kosovo: An IW Report Card", in Journal of Electronic Defense, (Horizon House Publications, August 1999, vol. 22, no. 8), p. 47-8.
[19] Department of Defense, "Kosovo/Operation Allied Force After-Action Report", Report to Congress, (Washington DC: General Printing Office, 31 January 2000), p. 6.
[20] Levien, p. 48.
[21] Daniel Verton, "DOD Redefining Info Ops", in Federal Computer Week, 29 May 2000, database on-line. Available from http://www.fcw.com/print.asp, p. 1.
[22] Ibid.
[23] Ibid.
[24] Department of Defense, "Kosovo/Operation Allied Force After-Action Report", p. 26.
[25] Verton, p. 2.
[26] Levien, p. 48.
[27] Maj. Gary Pounder USAF, "Opportunity Lost: Public Affairs, Information Operations, and the Air War Against Serbia", 19 April, 1999, database on-line. Available from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.htm, p. 12.
[28] Department of Defense, "Kosovo/Operation Allied Force After-Action Report", p. 51.
[29] Ibid.
[30] Daniel Verton, "Report Sheds Light on NATO's High-tech Problems in Kosovo", in Federal Computer Week, 9 February 2000, database on-line. Available from http://www.fcw.com/print.asp, p. 1.
[31] Pounder , p. 3.
[32] Joint Pub 3-13, p. II-1.
[33] Department of Defense, "Kosovo/Operation Allied Force After-Action Report", p. 55.
[34] Levien, p. 48.
[35] Cook, p. 5.
[36] Joint Command and Control Warfare Center, "Shortage of Perception Management Expertise", Joint Unified Lessons Learned System No. J5420-00076, 30 June 1999.
[37] Ibid., "Lack of Articulated Commander's Guidance Affected IO Planning and Support", Joint Unified Lessons Learned System No. J5420-00078, 29 June 1999.

[38] Maj Norman C. Davis USMC, "Information Operations and the Marine Corps Planning Process", in Marine Corps Gazette, (Quantico, VA), August 1998, p. 61.
[39] Bill Gertz, "Eligible Receiver", in The Washington Times, 16 April 1998, database on-line. Available from http://csel.cs.colorado.edu/~ife/114/EligibleReceiver.html, p. 1.
[40] "Eligible Receiver Exercise Shows Vulnerability", 22 December 1997, database on-line. Available from http://www.infowar.com/civil_de/civil_022698b.html-ssi, p. 1-2.
[41] Daniel Verton, "Whoops! War Plans Online", in Federal Computer Week, 1 May 2000, database on-line. Available from http://www.warroomresearch.com/mediapresenspeak/InterviewFCW4.htm, p. 1.
[42] Ibid.
[43] Jim Wolf, "High-Tech Firms Set Up Computer Defense Hub", Reuters News Service, 16 January 2001, database on-line. Available from http://dailynews.yahoo.com/h/nm/20010116/ts/tech_cybersecurity_dc_1.html, p. 1.
[44] Justin Pope, "Computer Company Challenges Hackers", Associated Press, 15 January 2001, database on-line. Available from http://dailynes.yahoo.com/h/ap/20010115/tc/hacking_contest_2.html, p. 1.
[45] LtGen. J.E. Rhodes USMC, "Information Operations", Marine Corps Concept Paper, 15 May 1998, database on-line. Available from http://www.concepts.quantico.usmc.mil/IO.htm, p. 11.
[46] Joint Pub 3-58, p. vi.
[47] LCDR Francis X. Sheehan USN, "Operational Deception and Modern Warfare: The Use of Deception in the Information Age", (Unpublished Report, US Naval War College, Newport RI: 8 February 2000), p. 13.
[48] Carl von Clausewitz, On War, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), p. 112.
[49] Douglas H. Dearth, "Information War: Rethinking the Application of Power in the 21st Century", in Military Intelligence, January-March 1997, p. 14.
[50] James F. Dunnigan and Albert A. Nofi, Victory and Deceit: Dirty Tricks at War, (New York, NY: William Morrow and Co., 1995), p. 372.

BIBLIOGRAPHY

Chairman of the Joint Chiefs of Staff. Joint Vision 2020 America's Military: Preparing for Tomorrow, Washington DC: General Printing Office.

Clausewitz, Carl, On War, edited and translated by Michael Howard and Peter Paret Princeton, NJ: Princeton University Press, 1976.

Cook, Nick. "Brain Storming", in Jane's Defense Weekly, 16 August 2000, database on-line. Available from http://homepage.mac.com/ebird1/s20000818/s20000818brain.htm.

Davis, Norman C. "Information Operations and the Marine Corps Planning Process", in Marine Corps Gazette, Quantico, VA, August 1998.

Dearth, Douglas H. "Information War: Rethinking the Application of Power in the 21st Century", in Military Intelligence, January-March 1997.

Department of Defense. "Kosovo/Operation Allied Force After-Action Report", Report to Congress, Washington DC: General Printing Office, 31 January 2000.

Dunnigan, James F. and Albert A. Nofi. Victory and Deceit: Dirty Tricks at War, New York, NY: William Morrow and Co., 1995.

"Eligible Receiver Exercise Shows Vulnerability", 22 December 1997, database on-line. Available from http://www.infowar.com/civil_de/civil_022698b.html-ssi.

Gertz, Bill. "Eligible Receiver", in The Washington Times, 16 April 1998, database on-line. Available from http://csel.cs.colorado.edu/~ife/114/EligibleReceiver.html.

Joint Command and Control Warfare Center. "Shortage of Perception Management Expertise", Joint Unified Lessons Learned System No. J5420-00076, 30 June 1999.

_____. "Lack of Articulated Commander's Guidance Affected IO Planning and Support", Joint Unified Lessons Learned System No. J5420-00078, 29 June 1999.

Joint Pub 1-02. The DOD Dictionary of Military and Associated Terms, Washington DC: General Printing Office, 23 March 1994 As Amended through 14 June 2000.

Joint Pub 3-13. Joint Doctrine for Information Operations, Washington DC: General Printing Office, 9 October 1998.

Joint Pub 3-58. Joint Doctrine for Military Deception, Washington DC: General Printing Office, 31 May 1996.

Levien, Frederic H. "Kosovo: An IW Report Card", in Journal of Electronic Defense, Horizon House Publications, August 1999, vol. 22, no. 8.

Pope, Justin. "Computer Company Challenges Hackers", Associated Press, 15 January 2001, database on-line. Available from http://dailynes.yahoo.com/h/ap/20010115/tc/hacking_contest_2.html.

Pounder, Gary. "Opportunity Lost: Public Affairs, Information Operations, and the Air War Against Serbia", 19 April, 1999, database on-line. Available from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.htm.

Rhodes, J.E. "Information Operations", Marine Corps Concept Paper, 15 May 1998, database on-line. Available from http://www.concepts.quantico.usmc.mil/IO.htm.

Sheehan, Francis X. "Operational Deception and Modern Warfare: The Use of Deception in the Information Age", Unpublished Report, US Naval War College, Newport RI: 8 February 2000.

Tzu, Sun. The Art of War, New York, NY: Oxford University Press, 1971.

Verton, Daniel. "DOD Redefining Info Ops", in Federal Computer Week, 29 May 2000, database on-line. Available from http://www.fcw.com/print.asp.

_____. "Report Sheds Light on NATO's High-tech Problems in Kosovo", in Federal Computer Week, 9 February 2000, database on-line. Available from http://www.fcw.com/print.asp.

_____. "Whoops! War Plans Online", in Federal Computer Week, 1 May 2000, database on-line. Available from http://www.warroomresearch.com/mediapresenspeak/InterviewFCW4.htm.

Wolf, Jim. "High-Tech Firms Set Up Computer Defense Hub", Reuters News Service, 16 January 2001, database on-line. Available from http://dailynews.yahoo.com/h/nm/20010116/ts/tech_cybersecurity_dc_1.html.