CANADIAN FORCES COLLEGE/COLLÈGE DES FORCES CANADIENNES

CSC 27/CCEM 27

EXERCISE/EXERCICE NEW HORIZONS

UNITED STATES INFORMATION WARFARE COMMAND - THE TIME IS NEAR

By /par Major Herbert Wesselman

April 2001

ABSTRACT:

The evolution of information warfare parallels the evolution of airpower in the first half of the last century. Although information warfare is not a new concept, it forms the basis of the current debate on whether or not a revolution in military affairs is occurring or has occurred. This paper explores the development of information warfare strategies and the legal implications of using information warfare weapons. It concludes that the individual efforts of the United States Armed Service need to be unified into a United States Information Warfare Command.

United States Information Warfare Command - The Time is Near

"To subdue the enemy without fighting is the acme of skill."
Sun Tzu[1]

History was made on December 13th, 1903 when the Wright brothers made the first powered flight at Kitty Hawk, North Carolina. Early aerospace power theorists like Gulio Douhet, Hugh Trenchard, and Billy Mitchell saw the potential of this new technology and advocated rapid technological improvements, development of new doctrine and establishment of new organizations to fully exploit the potential and revolutionize warfare.[2] In just over forty years the vast technological improvements, doctrinal developments, and combat experience, lead to the realization of Billy Mitchell's dream with the establishment of the United States Air Force in 1947.

Another historically significant event occurred on 15 February 1946 when ENIAC[3], the world's first electronic digital computer, was dedicated at the Moore School of Electrical Engineering of the University of Pennsylvania. The ENIAC was developed to speed up the preparation of firing and bombing tables for the US Army's Ballistic Research Laboratory at the Aberdeen Proving Ground in Maryland. This very first electronic digital computer with its thirty separate units and 19,000 vacuum tubes weighed in at over thirty tons, but provided the ability to compute a 60-second ballistic trajectory in 30-seconds, vice the 20-hours for a skilled person with a desk calculator. [4]

---

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971) 77.

[2] This generalization is derived from David R. Mets' monograph, *The Air Campaign.*

[3] ENIAC stands for electronic numerical integrator and computer.

[4] Martin H. Weik, "The ENIAC Story," http://ftp.arl.army.mil/~mike/comphist/eniac-story.html.

Although ENIAC was originally developed to help man wage war more accurately, it was not envisioned as a potential weapon of war. The progeny of ENIAC, however, are orders of magnitude faster, more capable, and interconnected to the point that today they are looked upon as potential weapons of war. In fact, information warfare using computers is at least ten years old with Iraq being its first target in 1991.[5]

Considerable debate revolves around whether or not the new information weapons and information warfare constitute a revolution in military affairs. David R. Mets defines three criteria for identifying a revolution in military affairs: a military technical revolution;[6] doctrinal concepts to take advantage of the change; and organizational changes to capitalize on the new technology and doctrine.[7] There can be little doubt to anyone currently in the military that information technology[8] has caused a military technical revolution since it is a critical part of almost every weapon and support system in use. The doctrinal aspects of a revolution in military affairs in the United States began to be addressed with the introduction of information superiority in *Joint Vision 2010*. The US Air Force has since promulgated *Air Force Doctrine Document 2-5, Information Operations* (AFDD 2-5) in August 1998. Organizational changes occurred as well. United States Space Command is tasked with both computer network defense (CND) and

[5] David A. Fulghum, and Robert Wall, "Combat-Proven Infowar Remains Underfunded," *Aviation Week & Space Technology*, 26 February 2001: 52.

[6] A military technical revolution as defined by David R. Mets is "…a rapid and large improvement in equipment used in combat and support of combat,…"(check additional citation rqmts)

[7] David R. Mets, *The Air Campaign, John Warden and the Classical Airpower Theorists*, (Maxwell Air Force Base, Alabama: Air University Press, 1999) 8.

[8] For the purposes of this paper information technology is used in a broad context to include computer systems, networks, and communications systems in common use in both the military and civil sectors.

computer network attack (CNA) missions.[9] Additionally, new organizations such as the Joint Information Operations Center, Air Force Information Warfare Center and units specializing in information warfare were established.

With the three conditions offered by Dr. Mets satisfied one could conclude that a revolution in military affairs has already occurred. However, the doctrine and organizational changes only scratch the surface of information warfare's potential. If used properly, information warfare has the potential to defeat an enemy without fighting and fulfill Sun Tzu's "acme of skill" vision. Realizing the full potential of information warfare requires further doctrinal development and organizational changes to develop mature employment strategies and an understanding of the legal implications of information warfare.

All of the US armed services are fielding information warfare capabilities. Similar efforts were underway in the 1980s with space systems and war fighting capabilities. These efforts were united when United States Space Command was established. As a result US military space efforts are highly integrated and provide a force multiplier unequaled in the world. Similar efforts need to be taken to integrate current service efforts in information warfare. Establishment of a United States Information Warfare Command will integrate current service efforts, and provide the United States with a credible information warfare combat capability.

This paper will explore rationale for establishing a United States Information Warfare Command. The rationale begins with developing an understanding of the difference between information-in-warfare and information warfare. An exploration of information warfare strategies will then demonstrate the potential of information warfare and a review of the legal

[9] Brendan P. Rivers, "Information Warfare: Where's the Action?" *Journal of Electronic Defense*, October 2000: 53-56.

ramifications of information warfare will show the need for establishing an organization solely responsible for the information warfare dimension. The final section is a description of the mission and command relationships of a future United States Information Warfare Command.

Information-in-Warfare/Information Warfare

> *"Attack where he is unprepared; sally out when he does not expect you."*
> SunTzu[10]

Information-in-warfare is defined in AFDD 2-5 as:

> … the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities. [11]

In short, information-in-warfare is knowledge of the enemy's strength, location, capabilities, and intentions. Information-in-warfare is not a new concept, but is as old as warfare itself. Proof lies in the final chapter of Sun Tzu's *The Art of War*. In this chapter, Sun Tzu states "Generally in the case of armies you wish to strike, … you must know the names of the garrison commander, the staff officers, the ushers, gate keepers, and the bodyguards. You must instruct your agents to inquire into these matters in minute detail."[12] Additionally, he states "And therefore only the enlightened sovereign and the worthy general who are able to use the most intelligent people as

[10] Griffith 69.

[11] *Air Force Doctrine Document 2-5 Information Operations* (Maxwell Air Force Base, Alabama: Headquarters Air Force Doctrine Center, 1998) 2.

[12] Griffith 148.

agents are certain to achieve great things. Secret operations are essential in war; upon them the army relies to make its every move."[13] The two passages above clearly show that even in ancient times information-in-warfare was vital to success in warfare. The only differences between ancient times and present day is the speed, sources, global scope, and quantity of information provided to commanders and civilian decision makers.

Information warfare is the second element of information operations as described in AFDD 2-5 and is defined as "…information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems."[14] The definition conjures up visions of sophisticated computer systems, networks, and skilled personnel protecting our vital information, and another group of equally sophisticated computers, networks, and personnel hacking into an adversary's information systems. With this vision in mind some may think information warfare is a recent conceptual development, the opposite is actually true. Again analysis of Sun Tzu shows that information warfare is as old as warfare itself. Even though Sun Tzu did not have computer systems, networks, or sophisticated collection platforms, he understood the value of information warfare when he stated "All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are near. Offer the enemy a bait to lure him; feign disorder and strike him."[15]

So, if information-in-warfare and information warfare are not new forms of warfare, why are they of such great interest to modern militaries? Andrew W. Marshall provides two observations to explain the increased interest in his foreword to *The Changing Role of*

[13] Griffith 149.
[14] AFDD 2-5, 2.
[15] Griffith 66.

Information in Warfare. The first is the growing dominance of long-range precision guided weaponry to destroy or disable the opponent's forces and support systems; resulting in defeat through the disintegration of command and control, instead of attrition or annihilation. The second is the increasing centralization of the information dimension to the outcome of conflicts.[16] Although militaries always have been dependent upon information-in-warfare, Marshall's first observation gets to the heart of why it is critical to warfare today. In a time when war fighters can target precision guided weapons and hit a window, door, chimney, or an equally discrete target, highly detailed information is required to achieve the desired results while minimizing collateral damage. As such information-in-warfare is a necessary element for all forces across the entire spectrum of conflict.

The more crucial observation, however, is Marshall's second. He continues the observation by stating that "…protecting the effective and continuous operation of one's own information systems and being able to degrade, destroy, or disrupt the functioning of the opponent's information systems will become a major portion of operational art."[17] This observation mirrors the AFDD 2-5 definition of information warfare. Further, he concludes "… early superiority in the information realm will become central to success in future warfare. It has always been important; it will soon be central."[18]

Now that "information" is becoming central to the success of future warfare, we must give it special attention to ensure its potential is not marginalized or overemphasized. A United States Information Warfare Command is required to provide the focus and to realize the full

---

[16] Zalmay M. Khalilzad, and John P. White, ed. *The Changing Role of Information in Warfare,* (Santa Monica, California: RAND, 1999) 5.

[17] *The Changing Role of Information in Warfare* 5.

[18] *The Changing Role of Information in Warfare* 6.

potential of information warfare. The first step for the new command is to develop strategies to effectively employ information warfare at the operational and strategic levels of warfare.

Information Warfare Strategies

> *Can the enemy insert false information, or corrupt the information given to you by your subordinates, to serve his purposes? Conversely, can you do the same to the enemy communications, assuming that they enjoy the benefits of the same means of electrical communications.*
>
> Thomas Jefferson[19]

The quotation above was taken from a letter Thomas Jefferson wrote to Benjamin Franklin in September 1784. It reveals how our forefathers contemplated the potential of information warfare 217 years ago. Now at the beginning of the 21st century, these same questions are the subject of considerable debate.

The proliferation of computers, the Internet and high-speed communications provides rapid information flow right to the personal computer in most homes and almost every office. The rapid flow of information also provides a new medium to attack the United States. Terrorist groups, non-governmental organizations, and individuals can corrupt, manipulate, and insert false information, or propagate malicious software on the Internet. Unfortunately, the bad information and malicious code travels just as fast as good information. Military systems, especially unclassified support systems connected to the Internet, are equally vulnerable.

The rapid worldwide spread of the "Melissa" and "I Love You" viruses highlights this vulnerability and the havoc even one individual can create. Fortunately, this vulnerability can be turned against an adversary to shape the future physical battlefield, or in some cases prevent actual confrontation between military forces. To understand how this vulnerability can be turned

[19] Alan D. Campen and Douglas H. Dearth, ed., *Cyberwar 2.0: Myths, Mysteries and Reality*, (Fairfax, Virginia: AFCEA International Press, 1998) 21.

against an adversary, a brief explanation of potential courses of action available to future adversaries of the United States and the information warfare strategies to counter them is required.

Brian Nichiporuk describes six asymmetric options that future adversaries may employ to negate the vast margin of military superiority of the United States in his contribution to *The Changing Role of Information in Warfare*.[20] In addition he details four information warfare concept of operations (CONOPs) to counter each asymmetric option as depicted in Figure 1 below. Although Nichiporuk provides detailed descriptions of the six enemy asymmetric options and the potential US responses, both sides of the figure can be simplified into three asymmetric options and three CONOP responses as depicted in the Figure 2.

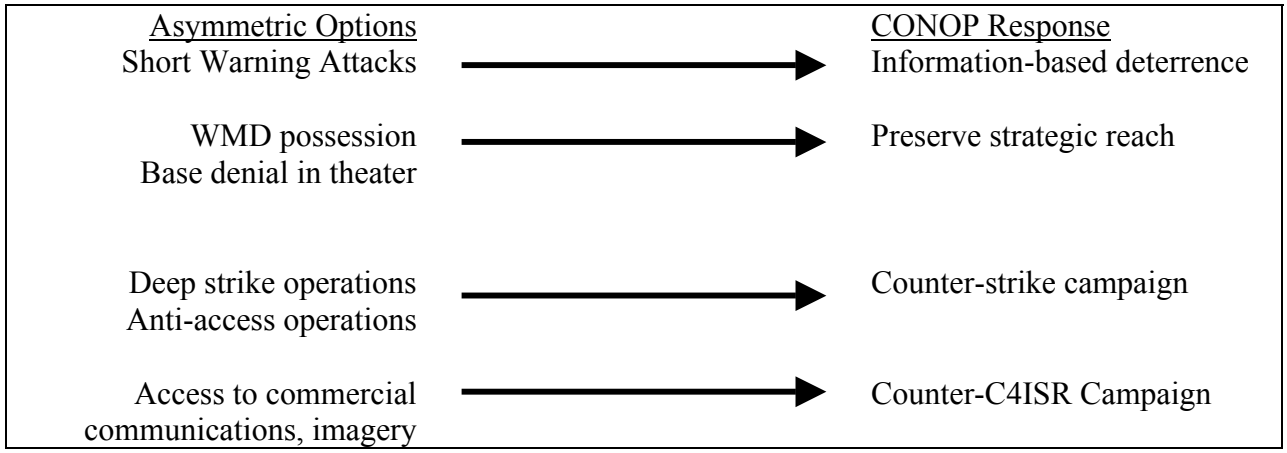

Figure 1 – Adversary Asymmetric Options and Potential US CONOPs[21]

[20] The section which follows relies heavily on the work of Brian Nichiporuk entitled "US Military Opportunities: Information-Warfare Concepts of Operations" included as part of *The Changing Role of Information in Warfare*. Additional detail on the asymmetric options and CONOP responses can be found in this article.

[21] Brian Nichiporuk, "US Military Opportunities: Information-Warfare Concepts of Operations," *The Changing Role of Information in Warfare* (Santa Monica, California: Rand 1999) 192.

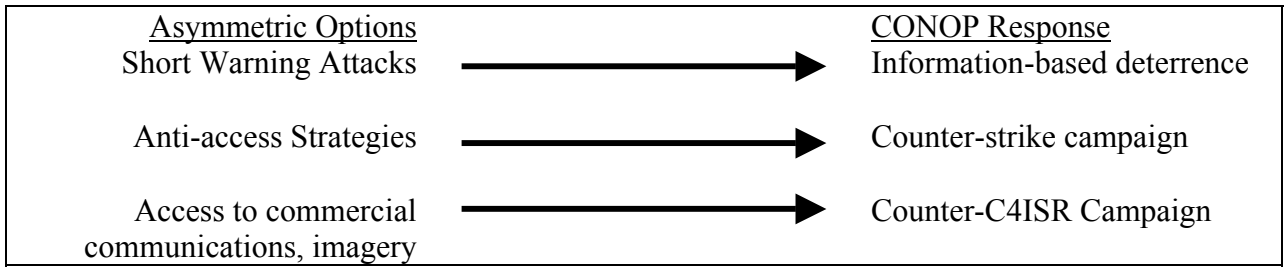

Figure 2 – Simplified Adversary Asymmetric Options and Potential US CONOPs

The initial invasion of Kuwait in August 1989 is a good example of a short warning attack. In short warning attacks, the adversary initiates hostile action with little or no warning to achieve his objectives and surprise his opponent. In the worst case scenario, the surprise attack will catch the opponent with few or no conventional forces in theater to respond to the hostile action. If the United States is the opponent or is an ally of the opponent, the short warning attack would force strikes or deployment of military forces from bases in the United States or a nearby theater of operation. In either case the risk to US military forces will be high, especially if the adversary possesses technologically advanced weaponry.

The best counter to this type of asymmetric attack is to prevent it from ever occurring. This requires deterrence similar to the nuclear deterrence which held the US and USSR back throughout the Cold War. The objective of an information based deterrence campaign would be to "sow doubt in the mind of a potential adversary about the likely outcome of his aggression.[22] In this way the United States can shape the aggressors reasoning about their intended course of action and dissuade him from acting. According to one Pentagon official recently quoted in the 26 February 2001 issue of *Aviation Week & Space Technology* "We're nearing the point where

[22] Nichiporuk 193.

we can manage the perception of the enemy. We want to influence the adversary to act in our interest without knowing they've been acted upon."[23] If the vision of "perception management" can be realized, information based deterrence will hold enormous potential by permitting the United States to prevent some conflicts from ever erupting into violent confrontation.

Nichiporuk's weapons of mass destruction (WMD), base denial, deep-strike, and anti-access options are consolidated to form the anti-access strategy, since they all seek to deny the United States the ability to deploy and utilize forces in a theater of operations. Anti-access campaigns can be accomplished using political, diplomatic, or military means as well as threatened use of WMD. Regardless of the method employed, the objective of the adversary is to complicate the potential military response of the United States and force adoption of a standoff approach to combat.[24]

An information warfare counter-strike campaign will best preserve the United States' ability to deploy and use military forces into a hostile theater of operations, and prevent having to fight a standoff battle. Information warriors would execute an information warfare counter-strike campaign by remotely attacking the adversary's command and control, planning and support systems. The intent of the remote attack would be to degrade, corrupt, or disable the systems the enemy depends on to execute his war plans. An example used by Brian Nichiporuk is an information warfare attack intended to degrade or neutralize portions of the adversary's integrated air defense system (IADS). Information warriors have several options to degrade, corrupt, or disable the IADS. These range from simple insertion or deletion of aircraft tracking information to a brute force shutdown of the entire system. When the information attack

[23] "Combat-Proven Infowar Remains Underfunded," 52.
[24] Nichiporuk 190.

commences on the IADS, air forces will be able to conduct operations in a significantly reduced threat environment.

There are two additional considerations for information warfare counter-strike operations. First, the counter-strike CONOP assumes hostilities have erupted, and the counter-strike is part of a coordinated joint campaign plan. The second is that a coordinated information warfare counter-strike attack poses less risk of conflict escalation with a WMD capable enemy, since the attacked system is not physically destroyed, leaving the adversary capable of defending itself at a later date.[25]

Information based deterrence and counter-strike CONOPs seek to shape the adversary's perception of events. The counter-C4ISR[26] campaign is the total war option for information warfare. As discussed earlier, the proliferation of computers, networks, and high-speed communications has created a highly complex and interconnected information environment. Commercial ventures are increasing their ability to provide satellite imagery, communications, and navigation systems. As a result, potential adversaries have greatly enhanced C4ISR capabilities that were only available to large, well funded military forces in the past. The objective of the counter-C4ISR campaign is to degrade the ability to use these commercially available and indigenous C4ISR capabilities by cutting off the information flow at key times in a campaign.[27]

Although the explosion of the Internet and commercial service providers provide a highly robust and redundant information network, it is possible to accomplish a counter-C4ISR

[25] Nickiporuk 200.

[26] C4ISR stands for Command, Control, Communications, and Computers (C4), Intelligence, Surveillance, and Reconnaissance (ISR).

[27] Nichiporuk 208.

campaign. The key to successfully conducting the campaign will be the targeting process. Similar to targeting of air power, detailed analysis must be done of the enemy's system to find the critical vulnerabilities, which if successfully attacked by information warfare would reduce or eliminate the flow of information into and out of his headquarters at critical moments. The lack of information will severely inhibit the enemy's decision process and will increase the fog of war for the commander. If the counter-C4ISR campaign is successful, the opposing force will act and react much slower to the changing operational environment and in extreme cases potentially cause paralysis in his forces. In other words "Counter-C4ISR is a potential war winner."[28]

All three of the above CONOPs show the combat potential of information warfare, from deterring conflict at one extreme, to winning conflicts at the other. Does the combat potential of information warfare justify creation a command solely responsible for conducting information warfare? Prior to considering the answer to this question, the legal ramifications of information warfare need to be analyzed.

Legal Ramifications of Information Warfare

> *"Subtle and insubstantial, the expert leaves no trace; divinely mysterious, he is inaudible. Thus he is master of his enemy's fate."*
> Sun Tzu[29]

In his article entitled "The Law of Cyberwar: A Case Study from the Future" included in *Cyberwar2.0: Myths, Mysteries and Reality*, Charles J. Dunlap, Jr. highlights four legal areas

[28] Nichiporuk 208.
[29] Griffith 97.

that must be considered in any information warfare campaign or operation. The first is whether or not the use of a computer weapon is an "armed" attack within the meaning of Article 51 of the United Nations Charter.[30] Dunlap's examination cites numerous examples where the use of computer weapons are not categorically "armed" attacks within the scope of international law. The one notable exception is the use of computer weapons that "…causes not only enormous economic damage, but also the loss of life."[31] In this case international law would view the attack as an "armed" attack, and permit the victim to use necessary measures of force to eliminate the threat.

The second legal issue considered by Dunlap is the status of individuals engaged in conducting an information warfare campaign or computer attack. Determining who is a combatant, noncombatant, or illegal combatant in the information dimension is not a trivial task. Making the determination first requires identifying the originator. In the case of the "I Love You" virus, it took the Federal Bureau of Investigation less than 24 hours to trace the attack to a single individual in the Philippines.[32] While the "I Love You" virus was an attack by a individual acting independently, a well organized attack by a state or terrorist group will probably take considerably longer to track due to additional resources available to these entities. Once identified, however, a judgment can be made on the individual or group's combatant status. State sponsored individuals or groups could easily be adjudicated as combatants. Terrorist and

[30] Charles J. Dunlap, Jr., "The Law of Cyberwar: A Case Study from the Future", Cyberwar 2.0: Myths, Mysteries and Realities (Fairfax, Virginia: AFCEA International Press, 1998) 141.

[31] Dunlap 141.

[32] Robert K. Ackerman, "Cyberthreat Increases with Technology Proliferation," *Signal* Dec 2000: 23-25.

lone individuals could be either noncombatants or illegal combatants. In either case, the response to the attack is a law enforcement matter vice an action requiring a military response.[33]

The final two areas Dunlap considered are targets and cyberweapons.[34] These two items must be looked at as a whole rather than two separate pieces. As with targeting of conventional munitions, information warfare commanders must select valid military targets and utilize weapons that do not cause collateral damage disproportionate to the military advantage gained as a result of the attack.[35] The complexity of current computer systems and the numerous interconnections between military and civilian networks makes the proportionality test extremely difficult. The difficulty arises from effects that cascade beyond the originally intended target. Cascading effects should be expected in all but the simplest attacks, and may be "…orders of magnitude greater and more complicated that those of bombs."[36] In the worst case, an attack against a technologically advanced adversary's military infrastructure may extend to the civilian infrastructure and cause mass civilian casualties. For instance an information warfare attack intended to disable an adversary's IADS, could make its way into the civilian air traffic control system if the two are interconnected as they are likely to be. As a result, civilian air traffic control systems could be disabled increasing the risk or causing fatal aircraft accidents.

Just as the potential for information warfare is enormous, the ramifications as described above are equally challenging. Establishing a United States Information Warfare Command will

---

[33] Dunlap 142-143.

[34] Cyberweapons is a term used by Dunlap to describe a variety computer attack weapons such as viruses and denial of service attacks.

[35] Dunlap 144.

[36] David Bond, "Uncertainties, Doubts Cloud Information Warfare Policy," *Aviation Week & Space Technology*, 26 February, 2001: 61.

enable the full exploitation of the potential. The next section describes this future command, its mission and command relationships.

United States Information Warfare Command

"Beginning in 2005, the probability of a cyber attack using state-sponsored capability gets very high."
Major General Bruce Wright
Commander, Air Intelligence Agency[37]

As discussed earlier, the responsibility for computer network defense (CND) and computer network attack (CNA) currently resides with United States Space Command. In addition, the Joint Information Operations Center and Air Force Information Operation Centers were established in recent years. The Air Force has gone further by establishing the 609th Information Warfare Squadron, and standing up additional information warfare flights for operational level commanders.[38] With information warfare already being assigned to a unified command and numerous organizations already established, why establish a separate US Information Warfare Command?

The previous discussions imply considerable expertise must be developed to fully exploit information warfare strategies and handle its ramifications. A unified command will permit focused development of a mature information warfare capability and strategies for its employment. Establishing a unified command to focus on one particular aspect of warfare is not without precedent. United States Space Command, United States Strategic Command, United States Special Operations Command, and United States Transportation Command are four

[37] Robert Wall and David A Fulghum, "Secrecy Shrouds Computer War Threat," *Aviation Week & Space Technology*, 26 February, 2001: 56.

[38] Robert Wall, "USAF Expands Infowar Arsenal," *Aviation Week & Space Technology*, 15 November, 2001: 102-103.

commands which focus on providing the National Command Authority and regional commanders-in-chief (CINC) with specific capabilities which are their sole responsibility. The mission of the United States Information Warfare Command would be to plan, advise, and execute information warfare campaigns on behalf of the National Command Authority or in support of a regional CINC.

Not all writers on information warfare are united behind the need to establish a US Information Warfare Command. Brian Nichiporuk, whose work formed the basis for the discussion on information warfare strategies stated that forming an "…information-warfare component commander…would probably be unwise, because it would only add another layer of command and control that could slow down U.S. and allied decision cycles."[39] Although an information warfare component commander would be appropriate if a separate information warfare service was established, it is not the case with a unified command. Under a unified command structure, CINC United States Information Warfare Command (CINCIWC) would be responsible for national level information warfare campaigns. At a theater level, CINCIWC would be responsible for providing an information warfare coordination center or liaison cell to the joint force commander. This would be identical to the way US Transportation Command and US Space Command integrate into a regional CINC's organization. Instead of being another level of command to slow down the decision cycle, the information warfare coordination center would provide the joint force commander with additional combat capability to strike targets.

In addition to providing additional combat capability to regional CINCs, United States Information Warfare Command could resolve two long standing information warfare issues. The first is the potential for conflict between intelligence gathering agencies and operators in the

[39] Nichiporuk 208.

military on the use of information warfare. The second is that military leaders will not trust or include technology or tactics into war plans that have not been tested and exercised under realistic conditions.[40]

Current information warfare capabilities and national intelligence methods and sources are both closely guarded secrets. Protection is accomplished by compartmentalization and limited distribution of information regarding these capabilities. This secrecy is a well publicized challenge facing intelligence gathering agencies and military operators. Rear Admiral John Johnson put it best when he was quoted in the 19 January, 1998 issue of Aviation Week and Space Technology, "We're always going to have a clash between those who want to read information and those who want to destroy it."[41] During the Persian Gulf War commanders read the e-mail of Iraqi commanders until the military was ordered to stop intercepting the message traffic. Later Air Force planners were permitted to destroy communications and command nodes with kinetic weapons, but not with information warfare tools or weapons.[42]

Creating a United States Information Warfare Command would permit closer integration between the agencies responsible for gathering intelligence and the military members responsible for taking military action against potential or known threats. Instead of intelligence agencies dealing with each individual service, the efforts of all would be coordinated by CINCIWC. This coordination of efforts would provide the intelligence agencies and military with a better understanding of each others requirements, and a forum for determining which requirement, listening or disrupting, has the highest priority during a conflict.

---

[40] David A. Fulghum, "Cyberwar Plans Trigger Intelligence Controversy," *Aviation Week & Space Technology*, 19 January 1998: 52.

[41] "Cyberwar," 52.

[42] "Combat-Proven," 52.

The second information warfare challenge that United States Information Warfare Command would resolve is developing trust in new technology and tactics. The initial fielding and use of the F-117 provides an interesting parallel to the current state of information warfare. In the case of the F-117 the leaders of NATO and European Command refused to use the aircraft in war plans unless it was exercised with the command in peacetime.[43] The F-117 has since proven to be a valuable asset in any war plan. Similar efforts must be undertaken if information warfare is to achieve its full potential. As Philip Odeen, then chairman of the National Defense Panel, stated, "We think it's important [to get them into the open enough] to do lots of testing and experiments. You can't just bring them [into a war] at the last minute and use them effectively."[44] Establishing the United States Information Warfare Command will permit the command to oversee the security requirements and remove of current security impediments that prevent information warfare weapons from being exercised in a realistic operational environment.

Conclusion

The evolution of information warfare parallels the development of airpower in the first half of the last century. Rapid technological advances required changes to doctrine and organizations to fully realize the potential of airpower. The formation of the United States Air Force in 1947 was the final realization that airpower was a revolution in military affairs. Although information warfare is not a new concept, the introduction of information technology inaugurated by the ENIAC in 1946 bought about rapid technological changes in the conduct of warfare. The rapid technological changes required development of new doctrine and

[43] "Cyberwar," 52.
[44] "Cyberwar," 52.

organizations to take advantage of information warfare's potential. Capitalizing on the full potential of information warfare requires a unified effort to develop mature employment strategies and an understanding of the legal implications of using information warfare weapons.

Is the time for a United States Information Warfare Command near? Sun Tzu wrote about warfare being based on deception and described how to shape the enemy's perceptions in his chapter on estimates.[45] Current visions of information warfare seek to shape the enemy's perceptions in much the same way by using strategies such as information-based deterrence, counter-strike campaigns, and counter-C4ISR campaigns. Information warfare is a potent weapon in the United States' quiver of military tools, just like space assets, transportation assets, sectial (pecatio

te(r)Tj12 0 0 1214746578723775.7578 Tmtat cCureeifiedcCom aners-in-chiefe mation warfarecComaR cpabmiliyr

BIBLIOGRAPHY

Ackerman, Robert K. "Cyberthreat Increases with Technology Proliferation." *Signal*, Dec 2000: 23-25.

Air Force Doctrine Document 2-5 Information Operations. Maxwell Air Force Base, Alabama: Headquarters Air Force Doctrine Center, 1998.

Bond, David. "Uncertainties, Doubts Cloud Information Warfare Policy." *Aviation Week & Space Technology*, 26 February 2001: 61.

Campen, Alan D., and Douglas H. Dearth, ed. *Cyberwar 2.0: Myths, Mysteries and Reality*. Fairfax, Virginia: AFCEA International Press, 1998.

Fulghum, David A. "Cyberwar Plans Trigger Intelligence Controversy." *Aviation Week & Space Technology*, 19 January 1998: 52.

Fulghum, David A., and Robert Wall. "Combat-Proven Infowar Remains Underfunded." *Aviation Week & Space Technology*, 26 February 2001: 52.

Khalilzad, Zalmay M., and John P. White, ed. *The Changing Role of Information in Warfare.* Santa Monica, California: RAND, 1999.

Mets, David R. *The Air Campaign, John Warden and the Classical Airpower Theorists*. Maxwell Air Force Base, Alabama: Air University Press, 1999.

Rivers, Brendan P. "Information Warfare: Where's the Action?" *Journal of Electronic Defense*, October 2000: 53-56.

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

Wall, Robert. "USAF Expands Infowar Arsenal." *Aviation Week & Space Technology*, 15 November 2001: 102-103.

Wall, Robert, and David A Fulghum. "Secrecy Shrouds Computer War Threat." *Aviation Week & Space Technology*, 26 February 2001: 56.

Weik, Martin H. "The Eniac Story." http://ftp.arl.army.mil/~mike/comphist/eniac-story.html.