STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DIGITAL DATA WARFARE TOOLS: SHOULD CINCs HAVE CONTROL?

BY

LIEUTENANT COLONEL HERB W. NEWMAN
United States Army

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Digital Data Warfare Tools:

Should CINCs Have Control?

by

Lieutenant Colonel Herb W. Newman
United States Army Signal Corps

DR. Steven Metz
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Herb W. Newman

TITLE: Digital Data Warfare Tools: Should CINCs Have Control?

FORMAT: Strategy Research Project

DATE: 15 March 1999 41 PAGES Unclassified

The meteoric explosion of information-age technologies led by the ongoing rapid evolution of cyberspace and microcomputers has brought about a revolution in Military Affairs. A new form of Information Operations (IO) Warfare, Digital Data Warfare, portends enormous ramifications for the national security of the United States, its allies, and potential coalition partners.

Joint Pub 3-13 provides doctrine for the execution of IO in joint operations. It discusses integration and synchronization of ***offensive*** and defensive IO in the planning and execution of combatant commanders' plans and operations to support the strategic, operational, and tactical levels of war. What Joint Pub 3-13 does not do is state that combatant commanders should have control of Digital Data Warfare tools.

This paper examines and answers important strategic questions concerning combatant commander's control and authority to employ offensive Digital Data Warfare tools. The guideposts of this study provide a primer for understanding control and employment of Digital Data Warfare.

TABLE OF CONTENTS

LIST OF TABLES

DIGITAL DATA WARFARE TOOLS: *SHOULD CINCS HAVE CONTROL?*

Flash, breaking news! CNN is reporting the U.S. military's usage of a new and previously top-secret weapon: a malicious computer code capable of attacking digital computer data. An unnamed high level Department of Defense (DoD) official has confirmed that this weapon, developed by some of the nation's brilliant digital data experts, was covertly introduced into North Korea's nuclear reactors causing them to safely shut down while simultaneously destroying their computer software. According to sources, this operation has severally degraded North Korea's nuclear weapons of mass destruction program without physical destruction of facilities and any loss of life. Additionally, this operation sends a powerful message to others that the US possesses this capability. Official spokesmen for both the Whitehouse and the Pentagon have refused to comment on the mission but a scheduled news conference is expected.

Although fictional, a scenario like the above is well within the possible and some might even say is one of the probable asymmetric attacks, this one cybernetic, the United States must be able to conduct and defend against. "The state of technology today makes the concept of using malicious computer code as a weapon very real. It is now possible to develop computer software viruses that target specific systems, to install the viruses covertly and then to have them operate in a manner that is advantageous and predictable to the attacker. There are no published incidents of computer viruses being used as a military offensive weapon in open source literature, but such attacks are not only feasible but probable."[1] Additionally, because of the United States' dominant military position, Americans are more likely to be the focus of numerous asymmetric strategies as weaker adversaries attempt to advance their interest while avoiding a direct engagement with the U.S. military. If forced into a direct conflict with the U.S., those same adversaries are likely to seek ways of leveling the playing field.[2]

One potential way of "leveling the playing field" is the use of Digital Data Warfare since today's modern societies are becoming heavily dependent upon information technology. Almost no business or element of society has remained untouched in this phase of the technological revolution. It is no surprise that a myriad of organizations and nation-states are investing in ways to attack this dependency on digital technology.[3] The National Security Agency (NSA) is the federal agency that concentrates on the use of information technology and focuses on the danger that renegades with computers pose to America's national security apparatus. The agency estimates that more than 120 countries now have offensive computer network attack capabilities that could be used in an attempt to seize control of Pentagon computers. The U.S. Department of Defense is no exception in its growing dependency on digital data, as well as its stated goal of conducting Information Operations aimed at affecting adversary information and information systems.[4]

In an effort military experts say is the start of the new information-age era in military conflict, the U.S. Joint Chiefs of Staff are adopting a new doctrine for conducting computer warfare. For the first time, offensive computer networks attacks will become an operational part of U.S. warfighting doctrine, and even could be used in peacetime operations.[5] Joint Pub 3-13, Joint Doctrine for Information Operations, states Offensive Information Operations encompass the integrated use of assigned and supporting capabilities to affect adversary decision makers and achieve or promote specific objectives. These assigned and supporting capabilities include operations security, military deception, psychological operations, electronic warfare, and ***may include computer network attack***.[6] Given this reality, what does this mean for the geographical and functional Commander-in-Chiefs (CINCs)? This is an important question because the CINCs are charged by the National Command Authority with accomplishing the National Military Strategy in support of the overarching National Security Strategy.

Should CINCs ***control employment*** of Digital Data Warfare (DDW) tools? If so, what DDW tools should they control and what authority should they have to insert and implement them toward accomplishment of the National Military Strategy? Though CINCs' involvement in Information Operations covers the spectrum from information relations with the media to direct kinetic weapon attack against information related targets, digital data warfare is the niche of focus.

DIGITAL DATA WARFARE

> ***The true aim is not so much to seek battle as to seek a strategic situation so advantageous so that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this.***
>
> ***B. H. Liddell Hart***

When Nazi Germany rolled its Panzer tanks into France in 1940, they were victorious against the numerically superior French forces because Paris had prepared to re-fight World War I, while Berlin incorporated the latest technology and tactics into their offensive. As the world focuses ahead to the next major conflict, the victorious side will be the one that realizes what the nature of this war will be.[7] Technology, combined with creativity by military thinkers around the world, is leading to the development and application of new forms of warfare.[8]

"Digital Data Warfare is malicious computer code covertly introduced into one or more specific computer systems or networks by an attacker to meet military, political, economic, or personal objectives."[9] It is important to view this weapon as a tool that the information warrior uses as a means to an end, not an end in itself. As with our earlier fictional scenario involving North Korea's nuclear reactors, the digital data warfare attack (means) was employed to significantly degrade North Korea's nuclear weapons of mass destruction program; a U.S. national strategic objective (end).

This new (or innovative modification of old) form of warfare defies traditional rules of time and distance, speed and tempo, and traditional military capabilities. Digital Data Warfare can attack key industries and utilities such as modern telecommunications and manufacturing, automated banking and finance systems, microprocessor based transportation and energy services, and government operations dependent upon data bases. Unlike the traditional overt attack, Digital Data Warfare is a covert campaign that can assist in overwhelming the functions of a modern society with the speed and employment time of an electronic connection from a global distance. Information warfare is not linear in nature; it has no front line. Potential battlefields are anywhere networked systems can be accessed.[10]

DIGITAL DATA WARFARE TOOLS, TYPES AND APPLICATIONS

Digital Data Warfare *tools* includes computer software codes used individually or in combination that target specific systems, for a specific objective, in a manner that is predictable to the attacker. These codes have the ability to attach themselves to computer software programs, replicate, reproduce themselves in other programs in the host or other networked systems, lay dormant until triggered, circumvent system security measures, and destroy themselves while eliminating all traces of its existence. Some of the known *types* of digital warfare tools take the form of computer pathogens or viruses such as logic bombs, time bombs, trap doors, Trojan horses, and worms (see table 1 for definitions).

Computer virus: Malicious computer code that attaches itself to another block of code in order to propagate. Viruses have the following components:

Self propagated mechanism. Must be able to move from one part of a system to another. Unlike worms, viruses cannot propagate beyond the host system without being downloaded or inserted.

Capability to replicate itself. A virus may not necessarily make copies of itself if it can fulfill its mission without replication, but it does have that ability.

Mission component. Must do something (usually something bad from the perspective of the system's owner)

Trigger. Must have a mechanism to set the virus off to do its mission. Computer viruses begin their lives as Trojan horses and some remain Trojan horses throughout their existence.

Flying Dutchman: A Trojan horse that erases all traces of itself after performing its mission. This is a common feature of Trojan horses that helps defeat subsequent investigation.

Logic bomb: A type of Trojan horse that may or may not be a virus. Its mission component is triggered by a true/false condition. Logic bombs do not propagate; they just sit and wait.

Malicious computer code: Any computer code that is on a system without the consent of the owner.

Time bomb: A subset of the logic bomb; its trigger is the date and/or time.

Trap door: A hidden software mechanism triggered to circumvent system security measures. This can be a legitimate programming technique that allows a developer to bypass lengthy log-on routines or access source code directly. Its existence, if known by unauthorized persons, however, can be the source of a significant security breech.

Trojan horse: Malicious computer code that is located within a desirable block of code (i.e., an application program, operating system software, etc.). To be a Trojan horse, the presence of the code must be unknown and it must perform an act that is unexpected by the owner of the system.

Worm: Malicious computer code, similar to a virus, can replicate itself. Worms are independent operating programs that can mail replicas of itself outside the host system. Worms may or may not have a mission component or a trigger.

Table 1 DEFINITION OF TERMS[11]

Digital Data Warfare is generally applied in five phases to accomplish predictable results that are predetermined by the attacker: ***penetration, propagation, dormancy, execution, and termination.*** Unclassified covert ***penetration phase*** techniques into the targeted system or network is achieved either through a peripheral device such as a printer, media such as a diskette, communications connection such as telephone or radio frequency path, electromagnetic pulses, and software programs either purchased or electronically accessed. During target penetration, the malicious code is concealed within a legitimate computer code of software or inserted into an infected component of the targeted system. An example involves the attack against the U.S. Air Force's Rome, New York Laboratory in 1994 when Air Force officials stated that hackers may have been working for a foreign country interested in obtaining military research data. Additionally, Air Force officials stated *the hackers might have intended to install malicious code in software for activation years later.* If successful, the malicious code could have possibly jeopardized a weapon system's ability to perform safely and even threaten the lives of the soldiers or pilots operating the system.[12]

Once penetration is accomplished, the ***propagation phase*** begins with the malicious code propagating its way through the system or network to locate its intended target. The target could be any of a number of system features such as software, hardware, files, databases, microprocessors, or separate nodes. The proliferation of integrated computer networks, many of which are local area networks (LANs) and wide area networks (WANs), offer pathways for the propagation of malicious computer code. Because of this linkage and information exchange, a network has to be more careful about computer viruses. You may be exposed to a virus although you practice safe procedures.[13] A well-known illustration of remote entry and propagation was documented in 1995. A Russian graduate student in St. Petersburg, Vladimir Levin, used sophisticated computer codes more than 40 times to break into Citicorp's computerized cash-management system. He transferred more than $12 million to banks around the world and had access to Citicorp's daily monetary transfer of $500 billion.[14]

Upon completion of penetration and target location, the Digital Data Warfare malicious code can lie dormant until the attacker's determined time of attack. The ***dormancy phase*** may be short such as that intended to simply disrupt a network or it could be prolonged to coincide with the attacker's other activities. "One of the advantageous properties of Digital Data Warfare is that weeks, months, or even years can elapse between the time the code is introduced into a system and the time it is triggered."[15]

When the Digital Data Warfare code's triggering mechanism activates the code, the all important ***execution phase*** begins and the code performs the attacker's objective of denial, degradation, deception, and / or exploitation. The triggering mechanism can be the system's clock, number of machine cycles, remote transmission of a RF signal, certain entered keystrokes such as a logon, or a routine communication request such as an aircraft to a ground station. One of the essential aspects of the execution phase is the malicious code's predictability in order to accomplish what the attacker set out to do.

The final phase of Digital Data Warfare application is the ***termination*** phase. Once the attacker has determined that the malicious code has accomplished its intended affect, the code may then destroy all copies of itself leaving no trace of its existence or affect. However, if the attacker determines that a second penetration would be difficult and the risks of compromising the malicious code's existence are worth it, the attacker may decide to direct the code back to its dormancy phase. Perhaps this explains the reported British discovery that American intelligence agents infiltrated the computer systems of the European Parliament and European Commission. Allegedly, these agents used Internet routers to access the parliament's internal network, taking advantage of the fact that American firms manufactured the systems' components. British officials claim that the American government used information from the electronic raid to assist them in the General Agreement on Tariffs and Trade (GATT). Despite a complaint by leaders of the European Parliament, no confession or even acknowledgement has been issued by the United States intelligence agency.[16]

Before moving ahead, it is important to note that Digital Data Warfare tools are an added component to other attack capabilities. Digital Data warfare tools may be employed unilaterally or in combination with other packages designed to achieve the attacker's desired objectives and affects. After penetration has occurred, the remaining phases of Digital Data Warfare are controllable and should be synchronized for highest payoff or shock value.

DIGITAL DATA WARFARE AT EVERY LEVEL OF WAR

The levels of war help to amplify and add clarity to activities by echelons within the theater across the full range of military operations. The levels of war (strategic, operational, tactical) provide a useful construct for ordering activities within AORs.[17] Each level is categorized by the outcome intended-not by the level of command or size of the unit.[18] Joint Pub 3-13, Joint Doctrine for Information Operations, asserts Offensive Information Operations may be conducted at all levels of war, inside and outside the traditional battlespace.[19]

Strategic Level - The level of war at which a nation, often as a member of an alliance or coalition, determines national or multinational security objectives and uses national resources to accomplish these objectives.[20]

Strategic level Digital Data Warfare is directed by the National Command Authority and may be aimed at all elements of an adversary's national power: political, military, economic, information. Strategic targets, such as the entire digital commercial infrastructure of a nation, may be attacked while minimizing devastation to the workings of a society or government generally associated with kinetic applications in conventional military operations. Strategic Digital Data Warfare may be planned or conducted by a combatant or subordinate commander within an assigned area of responsibility based on tasking by the National Command Authority.

Operational - The level of war at which major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or areas of operations. These activities encompass a broader dimension of time or space than do tactics.[21]

Operational level Digital Data Warfare is conducted by a combatant commander within the assigned area of responsibility, or the combatant commander may assign that responsibility to a subordinate Joint Force Commander (JFC). At this level, Digital Data Warfare can have strategic value and may help the Joint Force Commander seize and sustain the initiative and synchronize operational capabilities.

Tactical - The level of war at which battles and engagements are planned and conducted to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the precise arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.[22]

A service or functional component commander reporting to a JFC conducts tactical level Digital Data Warfare. The primary focus of Digital Data Warfare at this level is to deny, disrupt, destroy, or otherwise control an adversary's use of information and information systems. Targets include command, control, communications, computers, intelligence, and surveillance systems and other automated information-based systems related to conducting military operations.

COMBATANT COMMANDER CONTROL OF DIGITAL DATA WARFARE TOOLS

> *Nothing is more worthy of the attention of a good general than the endeavor to penetrate the designs of the enemy.*
>
> Niccolo Michiavelli

Combatant Commanders plan, rehearse, and conduct Information Operations in support of national goals and objectives.[23] They are to incorporate offensive and defensive Information Operations into deliberate and crisis action planning to accomplish their assigned missions.[24] Given this directive, the central question is whether combatant commanders should have control of offensive Digital Data Warfare tools and the authority to implement them in accomplishing the National Military Strategy. In order to answer this, we must consider several determining factors such as the target, injection authority, period of dormancy, triggering approval, and intended effects or results.

Strategic - The National Command Authority should have control over offensive Digital Data Warfare tools aimed at strategic level targets (elements of national power). The decision to inject, period of dormancy, and trigger Digital Data Warfare tools in strategic targets should remain at the highest national level since the intended effects or results are strategic in nature and could potentially have ramifications well outside of the combatant commander's AOR. An example would be the unexpected interruption or manipulation of a nation's civilian air traffic control system resulting in international airplane catastrophes killing hundreds of civilians.

Operational - Combatant commanders should have control over Digital Data Warfare tools aimed at operational level targets. Though the NCA should withhold authority to inject tools having operational level effects and decide the dormancy period, combatant commanders should have the authority to trigger these tools. Again, the intended effects or results are confined to the combatant commander's AOR. Digital Data Warfare at the operational level serves to accomplish theater strategic and/or operational objectives. An example would be the disruption of an adversary's lines of communications, logistics, command and control, and other related capabilities associated with organizing, commanding, deploying, and sustaining military forces.

Tactical - Combatant commanders should withhold control and injection authority of Digital Data Warfare tools while delegating triggering authority to service or functional component commanders assigned tactical mission responsibility. The dormancy period should be relatively short since Digital

Data Warfare at the tactical level is aimed at specific tactical objectives and the effects are confined to a certain tactical area of responsibility. An example would be the automated ranging computation of a weapon system or the command and control of troops in an engagement.

Control & Employment of Digital Data Warfare Tools

Type of DDW Code	*Authority to Insert Code - Authority to Use DDW for a Category of Targets*	*Authority to Trigger Code & Authority to use DDW*
Strategic Application Any Period of Dormancy	Commander-in-Chief	Commander-in Chief
Operational Application Long Periods of Dormancy	Commander-in-Chief	CINC
Tactical Application Short or no Dormancy	CINC	JTF Commander

Table 2 WHO SHOULD CONTROL EMPLOYMENT OF DDW [25]

Combatant commanders should control employment of operational and tactical level Digital Data Warfare tools, while the National Command Authority should withhold control of strategic level Digital Data Warfare tools. The determining factors in assigning control of Digital Data Warfare tools are the target, period of dormancy, and the intended level of war usage will impact; strategic, operational, or tactical. The decision to inject strategic and operational level targets and the period of dormancy should also be at the NCA level. Injection of tactical level tools should be controlled by the combatant commander, while employment of tactical level tools should be delegated to the service or functional component commander assigned the tactical mission.

WHY SHOULD CINCS HAVE CONTROL OF DDW TOOLS?

Combatant commanders should have control of Digital Data Warfare tools aimed at operational and tactical level targets for a number of reasons. First, combatant commanders are responsible to the National Command Authority for successful prosecution of theater level warfighting, achievement of strategic objectives within the theater of operations, and attainment of the decided military end-state.

Second, combatant commanders' contingency target folders are prepared during the CINC's planning process. Offensive Digital Data Warfare tools applied against selected operational and tactical level targets provides a unique application that the CINCs must have to execute full dimensional warfare.

Third, combatant commanders sequence operational level warfighting activities in order to achieve optimal effects. The authority to trigger operational level Digital Data Warfare tools is one of the sequencing activities used unilaterally or in combination with other aspects of military power.

Finally, Digital Data Warfare used in preparation of the battlespace and force on force engagements at the tactical level requires timely triggering of in-place malicious computer code. CINCs and designated Joint Force Commanders must have this authority in order to meet time constraints versus entering into a NCA approval process to trigger operational/tactical Digital Data Warfare.

DIGITAL DATA WARFARE CONCEPT AND DOCTINAL DEVELOPMENT

A major consideration in the control, triggering and usage of Digital Data Warfare is that of concept and doctrinal development. Questions surrounding responsibility for concept and doctrinal development, joint operations, and the role of the intelligence community are all valid considerations.

First, an overarching national policy, perhaps in the form of a Presidential Decision Directive governing the usage and combatant commanders' control of offensive Digital Data Warfare tools, is required. From this national policy directive, the appropriate concept and doctrinal development should be established and be the product of an interagency process inclusive of government and sectors of the commercial community capable of providing focused expertise.

Secondly, the organization responsible for concept and doctrinal development of CINCs' control of Digital Data Warfare tools must be uniquely capable of the requisite skill sets. Additionally, the organization must be situated within the Department of Defense (not a service) and be capable of integrating national-level warfighting capabilities, including those of the intelligence community.

Finally, I feel the National Command Authority should have a CINC as the responsible official for oversight of the concept and doctrinal development. Given today's Unified Command Plan (UCP) alignment, the Commander, United States Atlantic Command (USACOM) is the CINC with the intellectual resource, capable facilities, strategic location, and responsibility for evolutionary concept/doctrinal development for coherent joint operations. The Commander, USACOM would be an effective advocate for combatant commander control of Digital Data Warfare tools. He could do so via the Joint Staff, the Joint Requirements Oversight Council, the Joint Warfighting Capabilities Assessments, submission of CINC Integrated Priority List, the services and other CINCs.

DIGITAL DATA WARFARE AND THE NATIONAL MILITARY STRATEGY

In both the 1997 and 1998 *National Security Strategy* documents, the President integrates the strategic approach around the terms ***Shape, Respond,* and *Prepare Now.*** The nation's current military strategy is centered on these concepts and will provide the strategic direction of the Armed Forces over the next three to five years. It builds on the premise that the United States will continue to be globally engaged to **Shape** the international environment and create conditions favorable to US interest and global security. It emphasizes that U.S. Armed Forces must **Respond** to the full spectrum of crisis in order to protect the republic's national interest. It further states that as we pursue shaping and responding activities, we must also take prudent steps to **Prepare Now** for an uncertain future.[26]

Offensive Information Operations may be employed in peacetime to promote peace, deter crisis, control crisis escalation, or project power. The actual employment of offensive capabilities in these circumstances may require NCA approval with support, coordination, cooperation, and/or participation by other USG agencies. Military offensive IO must be integrated with other USG IO efforts to maximize synergy, to fully exploit capabilities and activities when needed, and to prevent confusion and fratricide.[27]

Author Brian Lewis states, "This author can muster no moral or ethical reasons as to why the U.S. should categorically exclude information warfare as opposed to other vehicles (e.g. diplomacy, conventional warfare, etc) for advancing U.S. policy. Information warfare is a decidedly remote form of confrontation and if executed correctly may very well permit the United States to avoid the conventional deployment of troops and munitions. It may be morally acceptable (especially in the age of the CNN televised war) to disrupt the enemy's information infrastructure, rather than bomb them into submission with weapons of destruction that lead directly to the loss of human lives, often citizens."[28] Though there are no intended human casualties when logic bombs destroy information infrastructure of another nation, they may cause significant collateral death, most likely among civilians.[29]

In applying Digital Data Warfare to the three concepts of the National Military Strategy (**Shape, Respond, Prepare Now**), we are reminded of the five phases of Digital Data Warfare: penetration, propagation, dormancy, execution, termination. We have seen that Joint Pub 3-13 directs that offensive IO (inclusive of computer network attack, which is termed Digital Data Warfare in this work,) may be employed in peacetime as well as war. It further establishes that IO may have their utmost impact on influencing an adversary decision maker in peacetime and the initial stages of a crisis.[30] Combatant commanders, with approval and direction from the NCA, should employ Digital Data Warfare in support of the National Security and Military Strategies. The following is one possible application of Digital Data Warfare's integration into the National Military Strategy.

Shape - Digital Data Warfare, with NCA approval, could be used as one component of the Armed Forces' inherent deterrent qualities. If approved, the penetration, propagation, and dormancy phases of Digital Data Warfare or computer network attack should be achieved prior to the onset of hostilities. By having malicious digital data code in an adversary's targeted automated system, the NCA has several options that may help prevent/reduce a conflict or perhaps deter aggression and coercion. Governments could use offensive digital data warfare to intimidate and pressure other governments just as they did with nuclear weapons, except that collateral damage in the physical sense will not be as great.[31] A second example to help illustrate the "shaping" attribute of Digital Data Warfare is Space Operations. In the same manner as products from intelligence satellites are used to support the shaping concept of the National Military Strategy, so could Digital Data Warfare. If conflict should occur, the "in place code" could serve to shape the battlespace by assisting in attacking strategic targets and achieving strategic surprise/deception.

Respond - Digital Data Warfare could be used to signal US resolve and commitment in an effort to limit a greater US response. After penetration, propagation, and dormancy are achieved, the malicious code could be triggered into the execution phase in order to accomplish a predictable result. This usage of Digital Data Warfare would be part or all of the US response. An example may be the corruption of financial accounts of a national level decision-maker or the financial systems of a nation itself. Another example would be when the objective is to paralyze the enemy's decision-making capability. The enemy's automated observation capability is either flooded with too much information, which his system cannot digest, or is subtly misled by planted false information.[32]

Prepare Now - Digital Data Warfare could be a key component of this concept. Joint Vision 2010 is the conceptual template for joint operations and warfighting in future conflicts. It provides the direction for the services' visions, thus ensuring

the future interoperability of the joint force.[33]
Joint Vision 2010's key enablers of information superiority and technological innovation provide the basis by which to transform the current concepts of maneuver, strike, protection, and logistics into the new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.[34] Digital Data Warfare supports attainment of information superiority which is the capability to collect, process, and disseminate an uninterrupted flow of accurate and reliable information, while exploiting or denying an adversary's ability to do the same.[35] Combatant commanders should make enhancement of Digital Data Warfare tools one of their Integrated Priority List (IPL) requirements.

RISKS AND COSTS

Incorporating usage of offensive Digital Data Warfare in accomplishing the United States' Military Strategy has some potential risks and costs. Several of the primary concerns center around risks and costs associated with reciprocity, perceived act of war, and world political opinion.

The United States is by far one of the world's most technically advanced societies and is highly dependent upon automation based technologies. This dependency poses a serious national security concern due to the vulnerability of America's critical information infrastructure to a devastating information warfare attack. According to testimony by the Director of Central Intelligence, Mr. George J. Trent, potential information warfare attackers range from national intelligence and military organizations to a host of others with criminal intent. As documented earlier in this work, over 120 countries are known to have offensive computer network attack capabilities and risk of reciprocity from any of these countries poses a danger if strong security measures are not adopted to counter computer network attack.

Another risk is that Digital Data Warfare intrusions may be interpreted as an act of war if discovered by targeted countries. Active computer network attack techniques border between internationally recognized espionage and what some countries consider an act of war. This risk poses additional concern in that information warfare capable nations will probably not openly declare war and attack the United States symmetrically but may use malicious computer code to asymmetrically attack through intrusion, tampering, disrupting, and potentially destroying critical information infrastructure systems.

Along with reciprocity and potential interpretation as an act of war, another risk and cost is that of world opinion. If the United States' peacetime usage of malicious computer against a sovereign state, especially an ally, were to be discovered and proven, condemnation by various international organizations could potentially damage the country's standing in the international community. The costs to America's moral and ethical position could be undermined and some countries, especially those considered anti-U.S., could use the proven discovery as a propaganda tool.

POLITICAL, LEGAL, AND CIVIL-MILITARY CONSIDERATIONS

> ***The political object-the original motive for the war-will thus determine both the military objective to be reached and the amount of effort it requires.***
>
> ***Carl Von Clausewitz, On War***

Digital Data Warfare must ultimately be viewed in a political context. The implications of its use, especially during peacetime, are matters for national level decision-makers to determine because of national security policy and legal considerations. Though this paper focuses on combatant commander's control and authority to employ Digital Data Warfare tools, a brief discussion of political, legal, and civil-military considerations is put forth.

POLITICAL CONSIDERATIONS

The pros and cons of employing Digital Data Warfare merit debate. Politically and strategically there are many attractions to state-sponsored offensive information warfare. It is relatively low cost, timely, not location specific, provides no early warning, is not forbidden, inflicts low human life costs, and can be waged in complete anonymity.[36]

Low Cost - As compared to the ever increasing costs associated with today's "smart and soon to be brilliant" conventional weapons, Digital Data Warfare would be relatively cheap to wage. Development and usage of malicious computer code could yield positive returns without enormous investment.

Timely and Not Location Specific - Penetration, propagation, and dormancy phases accomplished, Digital Data Warfare could be waged immediately regardless of target and attacker geographic locations. There are no early warning indicators.

Anonymity - Malicious computer code, if discovered and identified, has no identification characteristics. Covert employment and/or manipulation of the Digital Data Warfare tool is key to successful anonymity. Even if the code were compromised, it would be very difficult to conclusively hold someone or a nation-state accountable for the attack.

Minimal Loss of Life - Digital Data Warfare can be directed in such a manner as to minimize loss of human life. Attacks on resident data storage areas or corruption of information have the potential to be accomplished while causing minimal human casualties and structural damage.

National level politicians must consider deterrents to U.S. usage of Digital Data Warfare. Among technology dependent nations, there are several deterrents to waging information warfare. Factors such as economic interdependence, fear of escalation, and lack of technical expertise detract from the advantages of state sponsored information warfare.[37]

Economic Interdependence - According to economist, interdependence of the financial system is now formal because countries have vested interest in not letting the reserves of foreign currencies drop below a certain threshold.[38] Strategic and to some extent operational level Digital Data Warfare targeted at a nation's automated economic infrastructure could have negative effects on the U.S. economy due to the global linkage of financial markets.

Fear of Escalation - Digital Data Warfare could escalate to a conventional military conflict if the attacked nation could identify the perpetrator and held conventional military dominance or capability to respond. Additionally, escalation could be in the form of a reciprocal Digital Data Warfare attack if the attacked nation possessed the capability and judged the objective worthy of the risk. After all, this type of warfare degrades a nation's strength, destabilizes its economy, and threatens its autonomy.[39]

LEGAL CONSIDERATIONS

Legal implications surrounding the usage of Digital Data Network attack can be discussed in the context of the Law of Armed Conflict. Three basic principles central to the Law of Armed Conflict are the principle of military necessity, principal of humanity, and principle of chivalry. The principle of military necessity states targets must have a military goal and be consistent with the laws of war. The principle of humanity is concerned with proportionality in the type and degree of force used. The principle of chivalry deals with the use of trickery—both permissible ruses and impermissible perfidy or treachery. None of the principles present an absolute prohibition to the use of information warfare concepts, tactics or weapons, though each may limit certain implementations of the concept.[40]

Principle of Military Necessity - Permits the application of that degree of regulated force, not otherwise prohibited by the laws of war, required for the partial or complete submission of the enemy with the least expenditure of life, time and resources.[41] Digital Data Warfare can be employed in a manner to support operations aimed at limiting loss of human life and destruction of physical resources.

Principle of Humanity - Aimed at prohibiting the employment of force not necessary for the prosecution of war or for the partial or complete submission of the enemy with the least possible expenditure of life, time and physical resources.[42] The use of malicious computer code is generally not directed against people and thus would not be inconsistent with the laws of humanity. However, Digital Data Warfare could be employed in such a manner as to produce mass destruction and great loss of life that could be viewed in the comprehensive sense as inhumane. An example would be corruption of an airplane's navigational aids resulting in the catastrophic death of passengers and people on the ground.

Principle of Chivalry - Its premise is that warfighting should be done in accord with well-recognized formalities and courtesies.[43] Digital Data Warfare could be used consistent with recognized aspects of ruses, trickery, or misinformation.

Legal considerations governing the use of Digital Data Warfare are yet to be internationally agreed upon but the principles of military necessity, proportionality and chivalry can be carried forward. The specifics in how these general principles are to be applied to certain information warfare scenarios will likely require gradual refinement. As nations begin to agree on certain standards, these may well develop into a new international law. More immediate desires for regulatory guidance may prompt nations to seek agreement through the treaty making process.[44]

CIVIL-MILITARY CONSIDERATIONS

The U.S. military has a tradition of subordination to civilian authority. While the evolution of modern warfare continues to call for new applications of technology and military power, civilian control of America's military has remained a constant. Combatant commander control and usage of Digital Data Warfare tools, peacetime or conflict, is an example of an evolution in the application military power that does not weaken civilian authority over the military. One method of ensuring oversight of this process in the Chairmen, Joint Chiefs of Staff (CJCS).

Combatant commanders consider and use the CJCS as an advisor and information channel with the National Command Authority. As the senior military officer, the CJCS provides checks and balances between the military and civilian authority.

Combatant commander directed Digital Data Warfare operations would be accomplished under full knowledge of the CJCS and NCA review.

Finally, Congress routinely engages combatant commanders by way of congressional testimony and various reports. Combatant commanders' usage of Digital Data Warfare tools could be the subject of Congressional scrutiny and periodic review by the various armed services committees.

CONCLUSION

Combatant commanders should have control of some Digital Data Warfare tools while the National Command Authority should retain control over others. Digital Data Warfare tools aimed at ***operational*** and ***tactical level effects*** should be controlled by combatant commanders while those involving ***strategic consequences*** should be restricted to the National Command Authority. The overarching factor determining control over Digital Data Warfare tools is the level of war usage is to effect.

Authority to inject and trigger Digital Data Warfare tools is a second and third order affect of control. Though the National Command Authority should retain inject authority over operational level targets, combatant commanders should have the authority to trigger those operational level codes. Finally, combatant commanders should have the authority to inject and trigger tactical level Digital Data Warfare tools.

Word count = 5,826

ENDNOTES

[1] Lawrence G. Downs, Jr., Digital Data Warfare, Essays on Strategy XIII, National Defense University, Institute For Strategic Studies, National Defense University Press, Washington, DC, 1996, pg. 44.

[2] Patrick M. Hughes, Statement For The Senate Select Committee on Intelligence 28 January 1998, pg. 5, http://www.infowar.com/civil de/civil 022798a.html-ssi

[3] 7Pillars Partners, Infrastructural Warfare - An Introduction, pg1, http://www.7pillars.com/intro.html

[4] Graeme Browning, National Journal, Http://www.govexec.com/dailyfed/0497/042297b1.htm

[5] George I. Seffers, Joint Chiefs Inaugurate Information Combat Era, Defense News, November 9-15, 1998: pg. 1

[6] Joint Pub 3-13, Joint Doctrine for Information Operations, 9 October 1998, pg. viii

[7] Harvard International Review, ZAP! Information Warfare In The Next Century, Winter 1997/1998, pg. 1

[8] Patrick M. Hughes, Statement For The Senate Select Committee on Intelligence 28 January 1998, pg. 3 http://www.infowar.com/civil de/civil 022798a.html-ssi

[9] Lawrence G. Downs, Jr., Digital Data Warfare, Essays on Strategy XIII, National Defense University, Institute For Strategic Studies, National Defense University Press, Washington, DC, 1996, pg. 44

[10] Roger C. Molander, Andrew S. Riddle, Peter A. Wilson. Strategic Information Warfare - A New Face of War, National Defense Research Institute, RAND, Santa Monica, California, pg. xvii

[11] Lawrence G. Downs, Jr., Digital Data Warfare, Essays on Strategy XIII, National Defense University, Institute For Strategic Studies, National Defense University Press, Washington, DC, 1996, pg. 45

[12] Jean Guisnel, Cyberwars, Espionage on the Internet, Plenum Press, New York, N.Y., 1997, pg. 189

[13] Philip Fites, Peter Johnson, Martin Kratz, The Computer Virus Crisis, Van Nostrand Reinhold, New York, New York, 1989. Pg. 11

[14] Timothy L. Thomas, Deterring Information Warfare: A New Strategic Challenge, Http://call.army.mil/call/fmso/fmsopubs/issues/deteriw.htm, pg. 1

[15] Lawrence G. Downs, Jr., Digital Data Warfare, Essays on Strategy XIII, National Defense University, Institute For Strategic Studies, National Defense University Press, Washington, DC, 1996, pg. 51

[16] Brian C. Lewis, Information Warfare, Http://www.fas.org/irp/eprint/snyder/infowarfare.htm, pg. 3

[17] FM 100-5, June 1993, pg. 6-1

[18] Ibid., pg. 6-1

[19] Joint Pub 3-13, pg. II-9

[20] Joint Pub 3-13, pg. GL-10

[21] Joint Pub 3-13, pg. GL-9

[22] Joint Pub 3-13, pg. GL-10

[23] Ibid., pg. I-6

[24] Ibid., pg. I-5

[25] Lawrence G. Downs, Jr., Digital Data Warfare, Essays on Strategy XIII, National Defense University, Institute For Strategic Studies, National Defense University Press, Washington, DC, 1996, pg. 62.

[26] National Military Strategy; Shape, Respond, and Prepare Now…A Military Strategy for a New Era, September 1997, pg. 1

[27] Joint Pub 3-13, pg. II-8, II-9

[28] Brian C. Lewis, Information Warfare, Http://www.fas.org/irp/eprint/snyder/infowarfare.htm, Pg. 5

[29] Ibid.

[30] Ibid., pg. II-7

[31] Timothy L. Thomas, Deterring Information Warfare: A New Strategic Challenge, Http://call.army,mil/call/fmso/fmsopubs/issues/deteriw.htm, pg. 7

[32] K. Sundarji, Wars of the Near Future, To fight a new-style enemy, "information" weapons, http://www.pathfinder.com/asiaweek/98/0109/feat1.html, pg. 2

[33] National Military Strategy, pg. 17

[34] Ibid., pg. 17

[35] Ibid., pg. 18

[36] Matthew G. Devost, National Security In The Information Age, http://www.terriorism.com/documents/devostthesis.html, pg. 20

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] Robert W. Aldrich, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, *Information Warfare Series*, Institute For National Security Studies, U.S. Air Force Academy, Colorado, April 1996, pg. ix,x

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid

BIBLIOGRAPHY

Aldrich, Richard W., *"The International Legal Implications Of Information Warfare."* Colorado: USAF Institute for National Security Studies US Air Force Academy, 1996.

Arquilla, John and Ronfeldt, David F., *"CYBER WAR IS COMING!"* http://snyside.sunnyside.com/cpsr/nii/cyber-rights/library/Net-…/RAND-Cyberwar-is-Comin. 1993.

Arquilla, John J. and Ronfeldt, David F., *"Cyberwar and Netwar: New Modes, Old Concepts, of Conflict."* http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html. 1993.

Bishop, William Warner. *"International Law: Cases and Materials."* Massachusetts: Little Brown, 1971.

Browning, Graeme. *"Infowar."* http://www.govexec.com/dailyfed/0497/042297b1.htm. April 1997

Devost, Matthew G., *"National Security In The Information Age."* http://www.terrorism.com/documents/devostthesis.html. May 1995.

Downs, Lawrence G., Jr. *"Essays on Strategy, Digital Data Warfare."* Washington, DC: National Defense University Press, 1996.

Fites, Philip. and Johnson, Peter. and Kratz, Martin. *"The Computer Virus Crisis."* New York: Van Nostrand Reinhold, 1989

Freech, Louis J., *"Threats To U.S. National Security."* Statement before the Senate Select Committee on Intelligence, Washington, D.C., January 28, 1998 http://www.infowar.com/civil de/civil 022798b.html-ssi. January 1998

Guisnel, Jean. *"CYBERWARS Espionage on the Internet."* New York: Plenum Press, 1997.

Hughes, Patrick M., *"Global Threats And Challenges: The Decades Ahead."* Statement For The Senate Select Committee On Intelligence, 28 January 1998, http://www.infowar.com/civil de/civil 022798a.html-ssi. January 1998

Hundley, Richard O. and Anderson, Robert H., *"That Wild, Wild Cyberspace Frontier."* http://www.rand.org/publications/RRR/RRR.fall95.cyber/wild.html. 1994

"Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance." A Research Project for the: Chief, Information Warfare Division (J6K) Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon. Science Applications International Corporation (SAIC) Telecommunications and Networking Systems Operation, Contract No. MDA903-93-D-0019, 1995

"Infrastructural Warfare - An Introduction." http://www.7pillars.com/intro.html.

Johnsen, William T. and Johnson II, Douglas V. and Kievit, James O. and Lovelace, Jr., Douglas C. and Metz, Steven. *"The Principles Of War In The 21ST Century: Strategic Considerations."* http://carlisle-www.army.mil/usassi/ssipubs/pubs95/pow21/pow21p10.htm. November 1998.

Kirsch II, Robert A., *"Viruses And Computer Pathogens: Should DOD Care?"* Research Project. Carlisle Barracks: US Army War College, April 1997

Klinefelter, Stephen. *"The National Security Strategy And Information Warfare."* Research Project. Carlisle Barracks: US Army War College, April 1997

Lewis, Brian C. *"Information Warfare."* http://www.fas.org/irp/eprint/snyder/infowarfare.htm.

Mahnken, Thomas G., *"War in the Information Age."* Joint Forces Quarterly 19 Summer 1998

Makk, Laszlo. "The Level and Structure of power Delegated to High-Ranking Military Officials in a Democracy." Research Project. Monterey: Naval Postgraduate School, December 1997.

Molander, Roger C. and Riddile, Andrew S. and Wilson, Peter A., *"Strategic Information Warfare A New Face of War."* California: Rand, 1996.

Office of the Chairmen Joint Chiefs of Staff, "*Information Warfare: A Strategy for Peace…The Decisive Edge In War.*" Washington: 1997.

Office of the Chairmen Joint Chiefs of Staff, "*National Military Strategy of the United States of America - Shape, Respond, Prepare Now: A Military Strategy for a New Era.*" Washington: 1997

Okello, Fredrick. and Ayers, Richard. and Bullock, Patrice. and Erhili, Brahim. and Harding, Bruce. and Perdigao, Allan. "*Information Warfare: Planning The Campaign.*" Research Project. Air Command and Staff College, April 1996.

Partan, Matthew. "*Draft - Proceedings and Key Findings of an Asymmetric Warfare Workshop held November 24, 1998.*" Massachusetts: CENTRA Technology, Inc., 1998.

Perillo, Robert J., "*IW-D: Cybotage, Information Warfare - Attack (IW-A), CyberWar.*" http://www.infowar.com/class 2/class 022698a.html-ssi.

Peters, Ralph. "*Constant Conflict.*" Parameters Summer 1997.

Reisman, Micheal W. and Baker, James E., "*Regulating Covert Action: Practices, Contexts, and policies Of Covert Coercion Abroad In International And American Law.*" New Haven: Yale University Press, 1992

Richardson, Doug. "*Techniques And Equipment Of Electronic Warfare.*" New York: Arco Publishing, Inc., 1985.

Seffers, George I., "*Joint Chiefs Inaugurate Information Combat Era.*" Defense News, November 1998

Sexton, Joanne. "*A Combatant Commander's Organizational View of Information Warfare/Command and Control Warfare.*" Research Project. Newport: Naval War College, June 1995

Stein, George J., "*Information Attack: Information Warfare 2025.*" http://www.au.af.mil/au/2025/volumne3/chap03/v3c3-1.htm. August 1996

Stewart, Michael J., "*Information Operations, Information Warfare: Policy Perspectives And Implications For The Force.*" Research Project. Carlisle Barracks: US Army War College, April 1997

Sundarji, K. *"Wars of the Near Future."* http://www.pathfinder.com/asiaweek/98/0109/feat1.html. January 1998

Tenet, George J., Testimony before the Senate Committee on Government Affairs, Washington, D.C., 24 June 1998 http://www.cia.gov/cia/public_affairs/speeches/dci_testimony_062498.html

The White House, *"A National Security Strategy For A New Century."* Washington: 1997

Thomas, Timothy L., *"Deterring Information Warfare: A New Strategic Challenge."* <http://call.army.mil/call/fmso/fmsopubs/issues/deteriw.htm. 1997

"USACOM Major Focus Areas." http://www.acom.mil/acomweb.nsf/MFA?OpenNavigator

"Warfare in the information Age." Massachusetts: Institute For Foreign Policy Analysis, 1996

"ZAP! Information Warfare In The Next Century." Harvard International Review; Winter 1997/1998