NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

CYBERWAR AS ANTI-WAR:
THE KEYSTROKE IS MIGHTIER THAN THE SWORD

JOHN B. MAYS/CLASS OF 1999

COURSE 5602
FUNDAMENTALS OF MILITARY THOUGHT AND STRATEGY

FACULTY SEMINAR LEADER:
Lt Col Mark Clodfelter, USAF

FACULTY ADVISOR:
Dr. David Rosenberg

2 November 1998

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
02-11-1998		xx-xx-1998 to xx-xx-1998

4. TITLE AND SUBTITLE
Cyberwar as Anti-War: The Keystroke is Mightier than the Sword
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mays, John B. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
National Defense University
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Relates examples of wars in the past as wars to that utilize the power of information. Cyberwar is another powerful type of war that can be described as "actions taken during times of crisis or conflict (including war) to affect adversary information and information systems while defending one's own information and information systems." Computer network attack is a derivative of the commercial sector.

15. SUBJECT TERMS
IATAC COLLECTION; cyberwar

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	8	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	11/2/1998	Report 11/2/1998

4. TITLE AND SUBTITLE
Cyberwar as Anti-War: The Keystroke is Mightier than the Sword

5. FUNDING NUMBERS

6. AUTHOR(S)
John B. Mays

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Defense University

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

Relates examples of wars in the past as wars to that utilize the power of information. Cyberwar is another powerful type of war that can be described as "actions taken during times of crisis or conflict (including war) to affect adversary information and information systems while defending one's own information and information systems." Computer network attack is a derivative of the commercial sector.

14. SUBJECT TERMS
IATAC Collection, cyberwar

15. NUMBER OF PAGES
7

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

CYBERWAR AS ANTI-WAR:
THE KEYSTROKE IS MIGHTIER THAN THE SWORD

Kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without too much bloodshed [1]

Carl von Clausewitz discounts the pursuit of a bloodless war as misguided and doomed to defeat. After all, war's aim is to destroy the enemy's forces. How can this goal be accomplished without physical force or combat? Indeed, this rule "holds good even if no actual fighting occurs," when the enemy recognizes that defeat by combat is certain. [2] Yet when Sun Tzu states that "to subdue the enemy without fighting is the acme of skill," he is not referring to the threat of annihilation, but to an attack on the enemy's plans or strategy, what he calls the "supreme importance" in war. [3] All the generals in 500 BC didn't say "Amen," rather; "This is beyond our comprehension!" [4] Sun Tzu was clearly ahead of his time. Perhaps he should be translated as saying, "This aim is of supreme importance in war: an attack on the enemy's *information*." After all, when Clausewitz speaks of destruction of enemy forces, "nothing obliges us to limit this idea to physical force: the moral element must also be considered" – that is, the will of the enemy. [5]

We are further encouraged to avoid the costs and dangers inherent in

---

[1] Carl von Clausewitz, On War, ed and trans Michael Howard and Peter Paret (Princeton, NJ Princeton University Press, 1976), 75
[2] Clausewitz, 97
[3] Sun Tzu, The Art of War, trans Samuel Griffith (New York Oxford University Press, 1963), 77
[4] Sun Tzu, 77
[5] Clausewitz, 97

destroying the enemy by employing "other policies." The "other policy" we are proposing here is Information Warfare, primarily the notion of "cyberwar." Cyberwar involves conflict in the realm in which systems that operate in the electromagnetic spectrum – computers, telecommunications, etc. – interact. Information Warfare (IW) is defined as "actions taken during times of crisis or conflict (including war) to affect adversary information and information systems while defending one's own information and information systems."[6] In its broadest sense, IW comprises six components or pillars: psychological operations (PSYOP), electronic warfare (EW), operations security (OPSEC), deception, and computer network attack (CNA). With the exception of CNA, these are all traditional tools of warfare, both defensive and offensive. They can be used singly or in concert to prepare the battlefield for conventional attack. In the case of EW, there is even potential for violent, kinetic attack in the form of anti-radiation missiles (HARM). In fact, the destruction of a key enemy communications link could be construed as IW rather than purely strike warfare. CNA, the main component of what we define as cyberwar, is strictly offensive and has the widest range of subtlety and destructive effect – yet it need not be lethal. The great leap comes in suggesting that IW techniques alone can decide a conflict or win a war, and do so bloodlessly.

Through the ages, war theorists and practitioners have recognized that advances in technology permit new and innovative ways to wage war, even if

[6] Joint Staff/J7, Joint Publication 3-13, "Joint Doctrine for Information Operations"

changes in doctrine often lag changes in lethality. This phenomenon is especially true of cyberwar, which, like air warfare, introduces an entirely new medium to the battle – the realm of cyberspace. It is through this dimension, divorced from geography, that we may be able to stanch the bloody war of Clausewitz.

Secretary of Defense William Cohen puts modern information processing and command and control capabilities at the heart of the current revolution in military affairs.[7] DESERT STORM can be viewed as a precursor to the increasing predominance of information in war Although the techniques employed by the U.S. did not represent quantum leaps in technology, the glimmerings of cyberwar were evident in the strategy of disrupting Iraqi air defense communications. IW capitalizes on the growing sophistication, connectivity, and reliance on information technology. As a result of this interconnectivity, IW techniques can influence all three components of the nation-state: the people (P), the government (G), and the military (M) (figure 1).

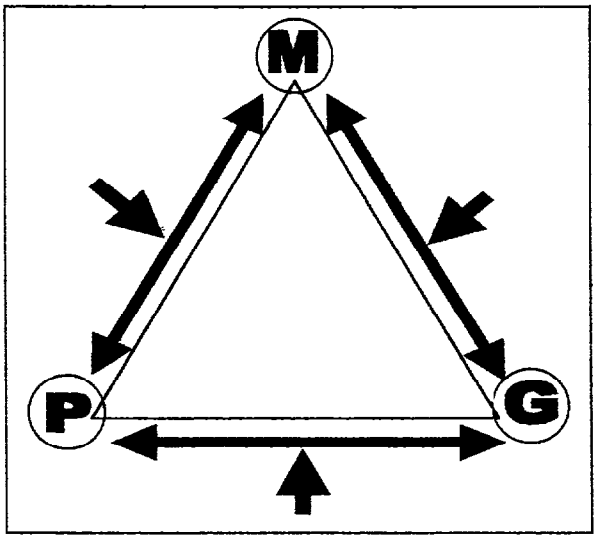

Figure 1

[7] William S. Cohen, Secretary of Defense, Annual Report to the President of the United States, (Washington, DC 1998), 118

The global connectivity that lends cyberwar its potency also necessitates a rethinking of actors and moral and ethical choices in its use. When is it exclusively a military application? Who wields the weapon if an attack on the financial sector is envisioned? Is it primarily a tool of nation-states, transnational groups, or individuals? Unlike most modern weapons, CNA technology derives from the commercial sector – it is the province of the hacker. When is first use or a preemptive strike allowable? Is a cyber attack an act of war? As implied in the example, the possibility of unintended civilian death is ever present. These questions surpass the debate over nuclear weapons, and underscore the truly unique nature of IW. The question that we seek to answer here is "If IW is a legitimate form of war, can it be non-violent? "

Current doctrine defines IW as an *integrating* strategy, designed to enhance the traditional tools of warfare rather than replace them. For the moment, there is little likelihood IW will assume the role of nuclear weapons in their early days, in the mistaken belief they had rendered conventional arms obsolete. There are also many parallels with the history of air power.[14] In its narrowest sense of war in cyberspace, IW grew up almost overnight. It has developed so rapidly, new practices and ideas become outmoded before they can be fully digested. Much of its doctrine is based on promise rather than practice. Finally, some would even propose establishing a separate "InfoCorps."

[14] Col Dave Tretler, USAF (Ret), "Air Power" (lecture given at the National War College, Washington, DC, 19 October 1998)

While this prospect is unlikely in the near term, IW is at least expanding from the Joint Staff (J6K) to the global CINC level of responsibility.

Does IW truly represent a revolution and not simply evolution in military affairs? Andrew Krepinevich defines a military revolution as "what occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase – often an order of magnitude or greater – in the combat potential and military effectiveness of armed forces."[15] Who would argue that the bloodless, non-lethal and asymmetric nature of cyberwar does not herald a fundamental alteration; or that the focused application of information in a computer network attack is not an exponential force magnifier?

Clausewitz wrote, "the invention of gunpowder and the constant improvement of firearms are enough in themselves to show that the advance of civilization has done nothing practical to alter or deflect the impulse to destroy the enemy, which is central to the very idea of war."[16] Does war in the Information Age negate this notion? I prefer to believe that the impulse survives, as borne out by the violent and bloody conflicts that still abound in the world. CNA, the essence of IW, brings war home to industrial man. It is as pervasive as the electromagnetic spectrum; its potency and reach increase with each new link established. It portends an era of nonviolent conflict. Yet

---

[15] Andrew Krepinevich, "From Cavalry to Computer," The National Interest No 37, Fall 1994, 30
[16] Clausewitz, 76

however effective it is or may grow to be, it cannot alter the physics of a bullet in flight. The "death machine" of conventional arms will proceed apace for the foreseeable future. As we navigate our way through the fog of the information revolution, we must seize the opportunity to shape its outcome.

> *"Victory smiles on those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."*[17]

[17] Giulio Douhet, The Command of the Air, trans Dino Ferrari (New York, NY Coward-McCann, Inc , 1942, rpt Washington, DC Office of Air Force History, 1983), 30