Chapter IV
Bits and Bytes vs. Bullets and Bombs:
A New Form of Warfare

John H. Nugent
University of Dallas, USA

Mahesh Raisinghani
Texas Woman's University, USA

... attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence. ~ Sun Tzu, The Art of War

There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind. ~ Napoleon Bonaparte

ABSTRACT

This chapter examines briefly the history of warfare, and addresses the likelihood that in the future wars may well be fought, and won or lost not so much by traditional armies and/or throw weights; but rather based upon digital offenses and defenses that are not constrained by geographic limitations or necessarily having overwhelming national resources. This changing landscape may well alter how nations or groups heretofore not a major threat to world powers, soon may pose an even larger threat than that posed by conventional weapons, including weapons of mass destruction (WMD), or at least approach parity with the destructive power of such weapons.

MACRO HISTORY OF WARFARE

The topic of warfare may be examined from different vantage points.

In examining warfare from various viewpoints, we see a progression from conflicts of a limited nature (scale, location, destructive power, etc.) to one where technology has mitigated to a large degree the linear

Figure 1. Historical analyses of warfare (Source: The University of Dallas Center for Information Assurance, 2005)

Warfare Defined

- By era or period
- By duration
- By scale or level of destruction
- By theater, geographic region, or weather
- By type (tribal, civil, extraterritorial, guerilla, declared, undeclared, hot, cold, etc.)
- By form (land, sea, air, space, Internet, some of or all five)
- By weapons, technology, or intelligence
- By national resources or national ages or stages
- By leader personalities
- By government forms or structures
- By strategies and tactics
- By drivers or reasons for, etc.

constraints of time, distance, and potential destruction. That is, where small groups, tribes or armies fought wars with weapons of a relatively limited capability in the past (pre-1945); today, we have powerful nations with significant resources that have strategic missile systems capable of delivering tremendous destructive power (nuclear, biological, chemical) virtually anywhere in the world at the push of a button in a matter of minutes.

The one constant in conflicts throughout the millennium has been that the victors almost universally were the adversary with the superior intelligence and command, communication, and control infrastructures (C3I). And while large nation-states have such strategic WMDs in their arsenals today, there is a new threat which all need to be cognizant of, that of the digital weapon where parties with significantly fewer resources than a super power may pose threats of an equally destructive nature. As James Adams has pointed out, "The United States may be the uncontested military superpower, but it remains defenseless against a new mode of attack: information warfare" (Adams, 2001).

No less than Nicholas Negroponte has pointed out that the nature of our assets is changing from the physical to the virtual (Negroponte, 1995). A sign of this fact is the growth in the amount of digital or digital information being stored today. Estimates of this growing volume of stored information ranges from one to two exabytes of new data a year, or approximately 250 megabytes of data for every man, woman, and child on earth (Sims, 2002).

Moreover, most systems, operations, and infrastructure today are run via digitally controlled systems ranging in degree of capability and security. Additionally, with technological advances in digital communications, most have come to recognize that telecommunications is a subset of information technology, and not vice versa.

Therefore, today our current state is such that our information base, control systems, and communications modes are all moving to a digital state that is even more interconnected. This movement creates a digital Achilles' heel where, the most digitally advanced party may also be the most vulnerable, or if adequately protected, possibly the most dangerous.

That is, "the anatomy of the Internet allows computer viruses [or other attacks] to spread much more effectively than was previously thought" (Pastor-Satorras, 2001). Moreover, the Internet lacks what Pastor-Satorras identifies as the "epidemic threshold," which in human terms naturally limits the spread of diseases across large segments of the population. And, "the very feature of the Internet that makes it so robust against random connection failures might leave it vulnerable to intelligent attack" (Barabasi, 2000).