THINKING OUT LOUD ABOUT CYBERSPACE (U)

by William B. Black, Jr.
Director's Special Assistant
for Information Warfare

INTRODUCTION (U)

one team, one mission

~~(S REL AUS CAN NZ UK)~~ On 3 March 1997, the Secretary of Defense officially delegated to the National Security Agency the authority to develop Computer Network Attack[1] (CNA) techniques. This delegation of authority has added a new, third dimension to NSA's "one mission" future. That is, in the networked world of Cyberspace, CNA technology is the natural companion of NSA's exploit and protect functions. This delegation of authority is sure to be a catalyst for major change in NSA's basic processes and its workforce. The end result, however, should remain information technology-derived products, services, and experts.

(U) The articles following this introduction were written by the staff of the Director's Special Assistant for Information Warfare. Because confusion still surrounds the emergence and history of Information Warfare (IW), these articles are intended to contribute to the common understanding of why Information Operations and its concepts are important to the future of NSA.

[1] DoDD 3600.1, Information Operations, dated 09 December 1996, defines CNA as "operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves."

A HISTORICAL PERSPECTIVE (U)

(U) After World War II, an understanding of the core competency underlying the making and breaking of codes — cryptology — resulted in a national decision to consolidate both activities in one organization: NSA. Both activities benefited from this consolidation, and became stronger.

~~(S REL AUS CAN NZ UK)~~Since the end of the Cold War, in an emerging networked world, an understanding of the emergence of a new core competency — "cyberology" — with its close technological relationship to cryptology has again resulted in a national decision to consolidate. Cyberology's central activities, i.e., "exploitation," "protection," and "attack," will be worked together, thus benefiting all of them.

SETTING THE STAGE (U)

(U) There are certain assumptions that underpin the thought processes related to preparing for our Agency's future in cyberspace. These are premises that are basic to the understanding, the preparations, and the acceptance of major changes. The following presents the main assumptions.

We're On the Edge of a New Age (U)

(U) First is an acceptance that we are on the edge of a new age, called the "Information Age." Also, that this new age is engulfing almost every aspect of society, including the very nature of our business. The basic premise is that the information technology advancements of the last 30 years far exceed any evolution of technology in the Industrial Age. These advances are so traumatic and far-reaching that they clearly represent something truly "new." It is important to note that, historically, technological advancements were called "revolutions" when they make progress of a single order of magnitude (e.g., the automobile "revolutionized" transportation because it was ten times faster than the horse). In the case of information technology, the contention is that the last thirty years have seen an advancement of not one but six orders of magnitude — 1,000,000 times! — in information technology. The end result has been a great deal of confusion and turmoil as human nature attempts to force the "new" of the Information Age into the "known" of the Industrial Age. This "new," however, does not fit; we have to change the thought process.

The Public Sees Government as the Bad Guy (U)

(U) Second, the public reaction to this new age has a direct relationship to the National Security Agency and the way we do business. At the beginning of the Industrial Age, the public centered in on industrialists and/or capitalists as being "the problem." Labor unions were created and child labor laws were enacted to curb their power. In today's Age, the public has centered in on government as "the problem." Specifically, the focus is on the potential abuse of the Government's applications of this new information technology that will result in an invasion of personal privacy. For us, this is difficult to understand. We *are* "the government," and we have no interest in invading the personal privacy of U.S. citizens. Regardless, the public's concerns are real and have an impact upon us. The Computer Security Act of 1987 is one example of this impact, for it clearly represents a first step in limiting any potential NSA involvement in the public sector.

This Age Brought Its Space With It (U)

(U) Third, a major aspect of the Information Age is that it is ushering in a totally new sphere of operations, a new environment called "cyberspace." For many, cyberspace is an ill-defined, comic-book concept — perhaps something created by a science-fiction writer or a Hollywood producer. But for NSA, in the Information Age, cyberspace is both real and virtual: while the real portion consists of physical assets (computers, network terminals, satellites, fiber optic cables, etc.) located on earth and in space, it is the virtual aspect — all interconnected, all networked, all compatible and interoperable — that is the most important. Almost every type of interaction that occurs in the physical world will have a corollary in cyberspace.

(U) In cyberspace, complex networks on networks emerge as an organizing concept upon which our future operations must focus. All networks are interconnected, and routing across the various elements of the network is automatic and not pre-determinable. Descriptors such as Defense Information Infrastructure (DII) or National Information Infrastructure (NII) refer to portions of users of the Global Information Infrastructure (GII) or better yet, the users of cyberspace's transportation system. The future global use and dependency on cyberspace should evolve much the way the use of the Internet has evolved today, i.e., because it should be extremely cost effective. The more important aspect of this inter-connectivity is the fact that, as we move into this complex networked future, computers are in charge, and physical geography becomes less and less important. While computers initially automated routine and mundane tasks, today inter-networking has turned computers and systems to networks, affording opportunities to work with greater and greater amounts of information at any distance. In the future, advances in artificial intelligence, and increases in understanding of cognitive processes, in general, will move us rapidly into a situation where computers and networks work in conjunction with each other, under broad guidance from humans, to actually make decisions and act on our behalf. This is cyberspace's future.

The Future of Warfare is Warfare in Cyberspace — a.k.a. Information Warfare (U)

(U) When we look to the future of warfare in the Information Age, we ask ourselves the question "How do you conduct warfare in cyberspace?" The answer is Information Warfare or, in accordance with DoD's new Directive 3600.1, Information Operations. Information warfare has been the subject of many speeches, scholarly papers, and popular journals. Information warfare has even made its debut in Hollywood in the film *Independence Day*. These many, differing views of IW confuse "information in war," "information technology enhancements of existing combat capabilities or weapon systems," and "warfare in cyberspace." In our view, "information in war" has been with us throughout history, i.e., intelligence on opposing forces was as valuable to Napoleon as it was to MacArthur. "Information technology enhancements" emerged during the Industrial Age with the natural evolution of weapons technology. IW for us, however, is "warfare in cyberspace" and is an exclusive feature of the Information Age. We believe that its biggest impact is yet to come.

(U) Another aspect of warfare that came with the Information Age is that actual, physical combat can be viewed in living rooms of America via television. The horrors of war cannot be hidden. As a result, in the simplest of terms, "body bags" are no longer acceptable. There is considerable societal pressure to find non-lethal means of accomplishing tasks that once called for conventional military action.

(U) For the military, the Information Age presents yet another problem. With the kind of computers, communications, and networking available in the commercial world, how can the military justify separate systems? Commercial communications networks are too inexpensive and too pervasive to ignore. The good news for the military is that — probably for the first time — they will have interoperable communications in joint service activities and even in multinational operations. The bad news, however, is that they will also be interoperable with their adversaries!

~~(S REL AUS CAN NZ UK)~~ In Information Age terms, IW provides a "digital coercion" option. The primary target of this option is the information infrastructure of an adversary. Such information infrastructures are expected to be primarily computer controlled, operated by the commercial-civilian sector (unprotected), and the primary infrastructure upon which military forces almost totally depend. For IW purposes, access to these computer-controlled infrastructures can permit the degradation, disruption, or destruction of the network and/or the functions they serve. As a result, the "computers" become the intelligence "targets" of highest priority.

~~(S REL AUS CAN NZ UK)~~ There are specific types of weapons associated with Information Warfare. These include viruses, worms, logic bombs, trojan horses, spoofing, masquerading, and "back" or "trap" doors. They are referred to as "tools" or "techniques" even though they may be pieces of software. They are publicly available, very powerful, and, if effectively executed, extremely destructive to any society's information infrastructure.

(U) As a last thought in setting the stage, we expect the Information Warrior of the future to be very different in their thought processes. They will understand the non-physical nature of the future capabilities, will be comfortable with working across the spectrum, and have extensive knowledge of non-military targets. Probably most importantly, they will be comfortable with the concept of networks. They will understand that "information operations" are more than "operations" supported by intelligence and communications; rather, they will understand that all three function together synergistically. Finally, Information Warriors will understand that in the "tooth-to-tail" accounting of personnel, military personnel will be the "tooth" and civilians will be the "tail." Tail equates to the emerging information infrastructure, a primary strategic target of IW.

THE BEGINNING (U)

~~(S REL AUS CAN NZ UK)~~ The following articles will look in depth at various aspects of Information Operations or Information Warfare as they relate to NSA. "Cyberology" and our new CNA mission should provoke much thought and discussion. It is hoped that these articles will serve as a catalyst and basis for these activities.

~~(FOUO)~~ *Mr. Black retired from NSA in 1997 after a long career. He was the first Director's Special Assistant for Information Warfare, and oversaw the establishment of the Information Operations Technology Center.*

KΛ