Editorial

By John T. Correll, Editor in Chief

Warfare in the Information Age

INFORMATION warfare has come upon us suddenly. It is true that the collection and use of intelligence are as old as warfare itself and that deceptive operations date back to the Trojan horse. It would be a serious mistake, however, to perceive what is happening now as a straight-line extension of the past.

When *Basic Aerospace Doctrine of the United States Air Force* was last published, in March 1992, it did not even include "information warfare" in the forty-page glossary. The closest it came to recognizing information warfare was to list surveillance, reconnaissance, and electronic combat as "force enhancement" missions.

Since then, the conceptual universe has shifted. One of the four major trends seen by Air University in "Air Force 2025" is that "influence increasingly will be exerted by information more than by bombs." In "Joint Vision 2010," the Joint Chiefs of Staff specify the central operational concept of the future—the one from which the others will flow—to be information superiority.

Gen. Ronald R. Fogleman, Air Force Chief of Staff, believes that "we're crossing a new frontier" and that information operations have now joined land, sea, air, and space operations as "the fifth dimension of warfare." In October, the Air Force identified information superiority as one of the service's six core competencies.

The change is driven by a combination of factors, including the advancement and proliferation of technology. Available computer speed, for example, doubles every eighteen months, making it possible to employ vast amounts of information at enormous speed. The postulated "Revolution in Military Affairs" is a self-reinforcing loop of global awareness, advanced command and control, and precision strike capabilities.

The Persian Gulf War of 1991 was a preview of things to come. Coalition airpower knocked out Iraq's command-and-control systems the first night. Coalition forces, receiving reconnaissance and signal data from aircraft and spacecraft, knew exactly what to do and when to do it. The advantage was overwhelming.

We are not yet altogether sure what information warfare is, much less what it means. Useful clues are found in "Cornerstones of Information Warfare," put out by the Air Force in 1995. It makes a distinction between *information age warfare*—which uses information technology as a tool in more or less traditional combat operations—and *information warfare*, which treats information itself as a weapon and a target.

The ultimate precision guided weapon is the electron.

So far, it is the first of these, information age warfare, that has gotten most of the attention. Leading elements of information age warfare are reconnaissance, surveillance, and battle-management systems in air and space.

The concept of information as a target and a weapon is less familiar. A Presidential commission is investigating the protection of critical national infrastructures ranging from telecommunications and financial networks to utilities, emergency services, and the continuity of government. (These infrastructures are starkly vulnerable. According to Glen Buchan of RAND, four of the Federal Aviation Administration's twenty air traffic control centers were closed for five hours when a farmer burying a dead cow accidentally cut a fiber optic cable.)

In March 1994, a sixteen-year-old hacker in London broke into the computer system of Rome Air Development Center, Rome N. Y., and acquired classified documents, which he then posted on the Internet. This year, an Argentinian hacker penetrated NASA and Department of Defense computer systems from his home in Buenos Aires.

According to Sen. Sam Nunn, who takes a special interest in this problem, about 250,000 attacks occur each year against unclassified but sensitive Department of Defense information systems. He says that perhaps sixty-five percent of these attempts are successful—and that we are catching only the least competent of the penetrators.

At a hearing in June, CIA Director John Deutch declined to respond in open testimony to a question from Senator Nunn about "whether foreign governments have indeed sponsored information attacks on our infrastructure." Senator Nunn speculated about an "electronic Pearl Harbor" in the offing.

The armed forces have a comprehensive stake in the problem, not only because more than ninety percent of their communications flow through commercial channels and because they rely on commercial databases but also because critical military advantages depend on information linkages. It has not escaped notice that when it comes to information attack, we are the world's fattest target.

Offensive information warfare entails a rich array of possibilities, but plans are screened by secrecy. Enemy radars and command-and-control systems—early targets in the Gulf War—would obviously be on the hit list in future conflicts. "Air Force 2025" looks beyond that to "prepositioned trapdoors" in computer programs and "cloaking devices and multispectral camouflage" but says "the most promising technology is the creation of synthetic environments that an adversary thinks are real." Taking it further still, Mr. Deutch told Congress that "the electron is the ultimate precision guided weapon."

Warfare in the information age carries us into uncharted territory. We will find new opportunities there, as well as dangers that we will not expect or fully understand. The objectives are not yet clear, and the problems we do see will almost certainly change before we can resolve them. The best we can do is to stay alert and flexible, equip ourselves with the best technology we can muster, and go forward with all the capabilities and options that we can muster. ■