INFORMATION ASSURANCE AND THE NEW SECURITY EPOCH

By Dr. John Hamre
Deputy Secretary of Defense

Protecting critical information resources will become "one of the defining challenges of national security in the years to come," says Deputy Secretary of Defense John Hamre. Noting that the Pentagon is charged with protecting 28,000 different computer systems, he warns that securing the virtual world from cyberthreats "is as much a process of management approach and attention as it is of technology."

The United States has faced five security epochs, with each change involving transitions from a certain past to an uncertain future. The first epoch was from the Revolutionary War to the mid-1820s, with the United States at the fringe of an international security environment still dominated by Europe.

From the mid-1830s to the end of the 19th century, we enjoyed the insulation of the Atlantic Ocean to tend to our own affairs as the old European political construct disintegrated. This second epoch ended with World War I and the emergence of the Soviet Union. A third epoch took place from 1920 to 1946 and was characterized by global recession and the rise of international communism as Europe collapsed. These events led to a crisis for American democracy and the free enterprise system with the Great Depression, and the tensions in the international security environment led ultimately to World War II.

The most recent epoch — the Cold War — was dominated by a bipolar world. The United States led the international community in creating institutions to rebuild the shattered economies of Europe and to deal with the collapse of the old Europe-dominated empires in the Third World. At the same time, the United States was leading the free world states to contain communism until the Soviet Union collapsed.

Now we are in transition to a new epoch, seemingly characterized by the revival of old dangers — nationalism and ethnicity. Another dimension in this new epoch is the dissolution of control and spread of the technologies that were created in the last epoch and the dramatic ascent of startling new technical capabilities that hold heretofore unheard of potential for both good and evil. We now live with the unsettling fear of "loose nukes" and chemical and biological weapons in the hands of terrorists.

The next security epoch also will present the challenge of cyber security. The explosive growth in the use of information technologies (IT) has had a profound effect on all sectors of the American economy and government. IT has fueled amazing economic growth, dramatically improved communications, and allowed American businesses to compete more effectively than ever. The United States — and the world — truly rely on information technology in ways unimaginable even just a few years ago.

Nowhere is this more true than in the U.S. military. The Department of Defense (DOD) is using IT to bring about what we call a Revolution in Military Affairs — the movement and use of vast amounts of information to provide more reliable intelligence, radically improved command and control, better business practices, and more powerful weapons systems. This revolution is vital if we are to remain ready to defend U.S. interests today and prepare for the evolving threat of the next security epoch.

The IT revolution is infusing every corner of DOD, both in the field and in the headquarters. Soon our soldiers at the squad level will have communications that allow commanders to know precisely the individual soldier's position, situation, and even heart rate — almost complete "battlespace awareness." Our sailors send e-mail home from ships at sea after using very similar technology to target cruise missiles. Pilots now factor in the "task saturation" of the flood of information available to them in flight.

In our logistics processes, technology is being used to connect the front lines to the supply lines. We are committed to a paper-free acquisition process by the turn of the century. We have opened our Joint Electronic Program Office to streamline unit-level purchasing and are now using Internet-based electronic "shopping malls" to buy everything from pens to hydraulic actuators. We are using the Internet for a spectrum ranging from travel payments to satellite communication, and we have made huge strides in electronic publishing.

In short, DOD is harnessing the power of the microchip to build the military of the 21st century. As we do so, however, we also must recognize that with new technologies come new dangers. The same technologies that allow us to seek new efficiencies can also be used by those who cannot attack us on the conventional field of battle to attack us in cyberspace. This is part of a very different and very important dimension in national security thinking; technologies and capabilities once accessible only to large nation-states are now accessible to individuals. The protection of our information resources — information assurance — will thus be one of the defining challenges of national security in the years to come.

There is little argument that information assurance is critical; we in DOD already have seen the first wave of cyberthreats in both exercises and actual attacks. To start to learn the extent of our vulnerabilities, last year we conducted an exercise. Our "enemy" was a group of about 35 people who had the mission to break into DOD computer systems. Their tools were limited to commercially available, off-the-shelf technologies and software that was sold on the open market or downloaded off the Internet. Within three months, the group, operating under those constraints, was able to attack us, penetrate our unclassified networks and, in fact, could have seriously disrupted our communications and power systems.

Last February, we experienced an organized attack against computer systems in the Pentagon at a time of increasing deployments to the Persian Gulf. It turned out to be by two teenagers in California, but coming when it did, the attack could have been much more serious. Both our exercise and small-scale attacks have served as wake-up calls that more serious attacks are not a question of "if," but "when" and "where."

To deal with these threats, we must first consider our mindset. Americans have traditionally thought of security like a fence around a yard, setting borders and protecting the area inside. If there is a break in the fence, it can be fixed and made secure again. This thinking worked well in previous security epochs, but there are no borders in cyberspace. The transition to the epoch to come must be marked not only by advancement of technology, but also by flexibility of thought. We must realize that security in the virtual world is as much a process of management approach and attention as it is of technology.

Changing mindsets can be among the most difficult of tasks. Without realizing it, we are now, for example, providing information to potential foes that they previously spent hundreds of millions of dollars in intelligence operations trying to acquire. We had one military installation with what was thought to be a great homepage on the Web. It showed an aerial view of the facility with buildings labeled "Operations Center" and "Technical Support Center." It was great public relations, but it also provided valuable targeting information for those who might wish us ill.

With an understanding of the broader issues involved with information assurance, we must move to take tangible action to protect our information resources. Within the past year, DOD has pulled together disparate efforts to try to understand the requirements to protect our information infrastructure. The pace of IT advancement makes this a daunting challenge; DOD has 28,000 different computer systems, all of them being upgraded and changed, and we must understand their vulnerabilities. The challenge of information assurance is akin to war, and we are approaching it that way by designating a Joint Task Force Commander for Computer Network Defense to organize our efforts. DOD is also a key contributor to the National Information Protection Center and the President's Critical Information Assurance Office.

Other actions are needed as well. Ninety-five percent of our communications are now over public telephone and fax lines, which makes encryption a core element in information assurance. One of the most dangerous scenarios in the virtual world is that our warfighters will receive deceptive "spoofed" messages that mislead them, so without reliable encryption, the entire information infrastructure on which we depend is vulnerable. In response to this threat, we are now working to ensure that within DOD, we can guarantee the digital identity of users and develop a reliable public key system. We must strengthen our encryption processes so that the information we transmit and deal with electronically is secure and verifiable.

DOD is also making important strides in broader network security. We are installing network monitoring capabilities and working to ensure configuration control over an inherently changing and dynamic network environment. We are installing firewalls, network monitoring centers, digital signatures, and a security infrastructure.

Information assurance, encryption, and network security pose some of the most daunting challenges the Department of Defense has ever faced. To take advantage of the IT revolution, we must ensure access to and protection of the very assets on which we depend. We are taking giant strides to make this happen, but much more remains to be done. These challenging days require that we turn to the expertise of information professionals both in DOD and in the broader government and private sectors to protect systems vital to all of us. We must ensure that our nation's journey into the new security epoch is as successful as the last.