Editorial

By John T. Correll, Editor in Chief

The Information Time Bomb

THE warnings keep on coming. In February, hackers launched a "distributed denial of service" attack against the nation's largest commercial Web sites, shutting off access to Amazon.com, eBay, Yahoo, E-Trade, and a number of others. For most of us, it was no more than a passing annoyance. Disruption of the Internet occurs often.

Even so, it is generally recognized that everything from the economy to continuity of the government depends increasingly on a starkly vulnerable electronic infrastructure.

The Department of Defense reports a rise in "cyber events" on its computer networks. It detects 80 to 100 attacks a day, of which about 10 are serious enough to get "detailed investigation."

Occasionally, an incident brings us up short. In January, the computers at the National Security Agency crashed suddenly and were down for three days. It was an internal glitch in the system, but at the time, NSA thought it might be under attack.

Call it another warning.

Contrary to the popular stereotype, not all hackers are teenagers or domestic malcontents. At least a dozen countries, perhaps twice that many, have information warfare programs directed at the United States.

Last year, angry about the NATO bombing of their embassy in Belgrade, the Chinese launched computer attacks on US government Web sites, including the White House site. In so doing, they blew the cover on clandestine "back doors" they had planted in US computer networks.

Nobody knows how deeply foreign powers have burrowed into critical US networks, siphoning off information or awaiting the time to strike. A nation with hostile intentions can do more than knock down Web sites.

It has been four years since Sen. Sam Nunn speculated about "an electronic Pearl Harbor." The phrase is repeated often, but we have not made much progress. A new kind of warfare is coming, and we are not prepared to meet it.

At an "anti-hacking summit" in February, the White House said the federal government would become a role model for computer security. At the moment, it has a ways to go.

A survey by the General Accounting Office finds computer security lax at most federal agencies. GAO penetrated mission-critical systems at NASA and said that "we could have disrupted ongoing command and control operations and modified or destroyed system software and data." At the Defense Department, the survey said, "pervasive weaknesses" offer abundant chances to modify, steal, disclose, or destroy data.

A new kind of warfare is coming. We are not prepared to meet it.

The problem does not suffer from lack of discussion. The White House has issued a "National Plan for Information Systems Protection," complete with numbered "milestones" and target dates. Congressional committees are holding hearings and drafting legislation. Industry has set up all sorts of councils and centers to promote computer security.

For all of the talk, there is little real coordination. The FBI has the lead for the federal government—to the extent that anybody does—but a law enforcement approach is not well-suited to either corporate or military requirements.

Security consultant Mark Rasch told *The Washington Post* that a successful case for the FBI means catching the perpetrator and holding a public trial. For business, success is thwarting the attacker so that he goes away and no one ever hears about it. The corporate world shows no enthusiasm for any government solution.

The Department of Defense has assigned the computer network defense and attack missions to US Space Command, but the armed forces have no charter to protect any computer systems except their own.

The Pentagon general counsel says that international law is unclear about when a computer network attack might constitute an "armed attack" or aggression against our national sovereignty. Our concept of operation is still in the definition phase.

The White House plan, which leans toward optimism, predicts that "our best efforts to identify and fix vulnerabilities will slow, but not stop, malicious intrusions into information systems."

By 2003, the plan says, federal networks should be able to recognize when an attack is in progress, spread the alarm, isolate the nodes that are under attack, and divert operations to alternate emergency systems. Meanwhile, "law enforcement and other agencies would be attempting to locate the origin of the attacks and take appropriate measures to terminate them," whatever that means.

That approach is geared to an attack on the Internet by hackers and criminals. A military attack on the national infrastructure would call for stronger measures, including more weight on the offense.

Part of the requirement is the development of new capabilities that do not now exist, but that may be the easy part. With investment and determination, the technology will come. The more difficult parts are organization and strategy.

Our military, civil, and commercial infrastructures are too interdependent to treat separately. Defending them will require integration of effort by defense, law enforcement, intelligence, and private participants on a scale not previously attempted, or even contemplated.

We must reach a firm decision that we will regard an attack on our national information infrastructures as an act of war. It must be totally clear that we will respond as surely and swiftly as we would to an invasion of our borders or to an attack on our forces.

Ambiguity is inherent in this new form of war, but that must not suggest to our adversaries that they might get a free shot. ■