

Defending Cyberspace

O. Sami Saydjari, Professionals for Cyber Defense

In February 2002, 54 information assurance professionals signed a letter to President George W. Bush expressing deep concern over the grave and growing risk to our nation from a threat potentially more devastating to the national psyche and economy than the 11 September 2001 terrorist attacks.

We observed that the country's critical infrastructure—including electrical power, finance, telecommunications, healthcare, transportation, water, defense, and the Internet—is highly vulnerable to cyber attacks. To avoid national disaster, we recommended that the president immediately form a Cyber Warfare Defense Project modeled on the Manhattan Project.

The White House's response was encouraging. Seven months later, it invited the group to review "The National Strategy to Secure Cyberspace" (<http://www.whitehouse.gov/pcipb/>), a draft for comment prepared by the President's Critical Infrastructure Protection Board. This invitation, coupled with the need for a formal organization to maintain an active role in the decision-making process, led to the formation on 18 September of Professionals for Cyber Defense (<http://www.USPCD.org>).

PCD's goal is to help the US government form a sound cyberspace defense policy. Intended to be small and focused, the nonprofit group consists of approximately 30 nationally recognized technical leaders in the field from industry, government, and academia, with rotating leadership. PCD is unique in being the only cyber advisory group whose



A strategy to deal with cyber attacks against the nation's critical infrastructure requires first understanding the full nature of the threat.

members act individually as concerned citizens rather than represent their particular sector's special interests.

On the same day of its formation, PCD created a panel specifically to examine the White House draft. It inferred from the document that the US government currently sees no urgent national strategic threat to the nation's critical information infrastructure. This premise seems to be based on the questionable notion that commercially motivated best practices can sufficiently address the problem.

Although the plan offers valuable advice to counter lower-grade threats, its underlying premise is at odds with the conclusion of several distinguished scientific bodies—including the President's Commission on Critical Infrastructure Protection, National Academy of Sciences, and US Defense Science Board on Information Warfare Defense—that a clear and present danger exists.

We acknowledge that these studies were based solely on the best collective judgment of the scientists involved. To date, no definitive research and validation process has been conducted on the national vulnerability. This failure to establish the full nature of the problem

represents a fundamental flaw in the White House strategy.

PCD recommends that President Bush promptly initiate a scientific process to assess the scale and gravity of the strategic threat of cyber warfare against the US. We expect it will confirm repeated warnings from the technical community.

Assuming that such a process affirms a serious national threat, we urge the federal government to

- assume a strong defensive role against serious attack,
- focus on countering strategic attacks having real-world effects,
- develop a top-down architecture and engineered approach to the problem,
- acknowledge that current technology is insufficient to defend against cyber warfare, and
- subsidize critical private defenses.

We believe these recommendations must ultimately lead to an aggressive program involving the commitment of both private and public resources.

The stakes are too high for an ambivalent response to the danger of large-scale cyber attacks—the scientific community and government must work together to define the danger and determine the best course of action before it is too late. ■

O. Sami Saydjari, current leader of Professionals for Cyber Defense, heads the Cyber Defense Agency, a research company and consultancy based in Wisconsin Rapids, Wisc. Contact him at ssaydjari@CyberDefenseAgency.com.