

23 December 2008

By: Lucian Constantin, Web News Editor



U.S. is not ready for cyber-attacks
NASA Jet Propulsion Laboratories

[U.S. Computer Security Policies are Unfit for Cyberwar](#)

This is the result of a large-scale cyber-attack simulation

Over 200 representatives of numerous U.S. government institutions and agencies, as well as private firms and computer security research groups, participated in a two-day long exercise that simulated the launching of and defending against a sustained cyber-attack. The results outlined that the U.S. was not even close to being ready for a potential cyberwar.

The participants were split into two groups - the attackers and the defenders. The former faction had to develop tactics that would have allowed it to disrupt the activity of vital computer networks serving critical infrastructure systems, while the latter had to rely on its past experience and known policies in order to successfully mitigate the cyber-assaults.

The simulation revealed significant problems in planning, establishing leadership and efficient communication. "There isn't a response or a game plan. There isn't really anybody in charge," Mark Gerencser, the vice president of Booz Allen Hamilton consulting service, the company that organized the exercise, commented, according to [The Register](#). This is consistent with the findings of the Center for Strategic and International Studies, which recently released a report for the Obama administration that recommended naming a White House assistant to oversee and coordinate cybersecurity efforts.

Attacks launched over the Internet in order to cripple critical systems are likely to become a common practice in the future of warfare. After the exercise, officials reminded of similar attacks originating in Russia, that hit Estonia, [Lithuania](#), and [Georgia](#) in the last two years. Democratic U.S. Rep. James Langevin of Rhode Island described the current state of things as similar to the one before September 11, when no one was ready for an incident like that one.

Michael Chertoff, the secretary of Homeland Security, suggested that computer security had been ignored or poorly treated for too long, even though computer networks played a key role in managing everything from banking to electrical systems. "We know that if someone shoots missiles at us, they're going to get a certain kind of response. What happens if it comes over the Internet?," he asked rhetorically.

Cyberwars are real scenarios, if we consider that cyber espionage is already a common occurrence. South Korea [pointed the finger](#) at its communist cousins from the north more than one time for hacking into its systems in order to gather Intel. The computers of several U.S. government agencies have been [compromised](#) by hackers [numerous times](#) over the years. This year alone, the [Pentagon](#) and the [White House](#) networks have been attacked by Chinese hackers, while an information-stealing worm has [spread](#) over both the unsecured and secured U.S. Military networks.