

## US cyber exercise providing valuable lessons: officials

September 30 2010

---



Analysts at the National Cybersecurity & Communications Integration Center (NCCIC) prepare for Cyber Storm III during a media session at their headquarters in Arlington, Virginia, on September 24. US cybersecurity experts will learn valuable lessons from an ongoing exercise that simulates a massive cyberattack on the United States, US officials said Wednesday.

US cybersecurity experts will learn valuable lessons from an ongoing exercise that simulates a massive cyberattack on the United States, US officials said Wednesday.

"Cyber Storm III," which simulates a "large-scale [cyberattack](#) on [critical infrastructure](#)," kicked off on Tuesday and involves thousands of participants in the United States and a dozen other countries.

"I can say that we are very pleased with how things are going," said Phil Reiting, a deputy undersecretary in the [Department of Homeland](#)

[Security](#) (DHS), which is organizing the three-day exercise.

"Exercises of this type give us a real window into what the capabilities are, where we need to make progress," Reitingger told reporters at US Secret Service headquarters here, where the "exercise control room" is based.

"One of the things that's critical to recognize about cyberspace is this is beyond the capability of any one government agency to respond to, or even one government or one private sector entity," he said. "This really requires a joint response."

Reitingger said the exercise is a test of the "ability to tie together information across sectors, across the government, with the private sector and internationally and generate a common response."

Seven US government agencies are taking part in the exercise, 11 US states, 60 private companies and 12 international partners: Australia, Britain, Canada, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Sweden and Switzerland.

Reitingger, a former Microsoft executive, said the exercise is the first opportunity to test the new National Cybersecurity and Communications Integration Center (NCCIC) based in Virginia.

The NCCIC booted up in October 2009 to serve as the coordinating center for US cybersecurity operations. It houses US [government computer](#) experts and their private sector counterparts under one roof.

"We had other mechanisms before, we had other bodies," Reitingger said.

"What NCCIC provides is the organizational mechanism to bring all of those capabilities together on a joint watch floor, to share information

not only virtually but between people breathing the same air."

After the exercise ends, officials are due to draft an after-action report whose conclusions will be integrated into the national response plan.

Brett Lambo, director of DHS's Cyber Exercise Program, described the exercise as "an organic, living breathing thing."

"Everybody's fighting the same core scenario" and trying to make it as realistic as possible, he said.

"We certainly hope we're minimizing the loss of fidelity as to what a real event would look like."

According to DHS officials, the scenario for the exercise involves a simulated cyberattack on government and private networks that undermines basic trust in the Internet.

(c) 2010 AFP

Citation: US cyber exercise providing valuable lessons: officials (2010, September 30) retrieved 27 April 2024 from <https://phys.org/news/2010-09-cyber-valuable-lessons.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--