Two years and 100 mln dollars buys winning cyber army

August 1 2010, by Glenn Chapman

People attend a conference on cyber security. A computer espionage specialist has laid out blueprints for building a cyber army capable of crashing through US defenses. Readying an unstoppable Internet invasion would take two years and a total of 100 million dollars, according to Charlie Miller, who spent five years with the US National Security Agency under then-director Michael Hayden.

A computer espionage specialist has laid out blueprints for building a cyber army capable of crashing through US defenses.

Readying an unstoppable Internet invasion would take two years and a total of 100 million dollars, according to Charlie Miller, who spent five years with the US National Security Agency under then-director Michael Hayden.

Now a researcher with Baltimore-based Independent Security Evaluators, Miller on Saturday shared his battle plan with hackers at a

DefCon gathering in Las Vegas.

"I pretended [North Korea](#) asked me to scope out the job of orchestrating a [cyber attack](#) on the United States," Miller told AFP. "I lay it out as I would do it realistically."

Miller explained that he had actually been asked by the Cooperative Cyber Defence Centre of Excellence in Estonia to play general in the theoretical attack scenario.

He shared his results at a NATO briefing in that country in June.

"I already knew it was easy, but now I know in detail how easy it would be," said. "We are certainly very vulnerable."

Miller described the 100-million-dollar price tag as a bargain compared to how much money is spent on [cyber defense](#).

He crafted a broad strategy to target smart grids, banks, communications and all other aspects of a nation's [technology infrastructure](#).

The cyber army would number about a thousand soldiers ranging from elite computer commandos to basic college trained geeks, according to the plan.

A key to success was stealthily breaching networks and establishing beachheads in computer systems during the two years before the main cyber invasion.

"Once you give me two years to get set up you are basically screwed," Miller said. "But, during the two years you have the opportunity to see what is going on and stop it before it gets going."

Miller determined that single targets, such as stock market or military networks, could be attacked much more economically.

North Korea was used in the war scenario on the premise that it has a tactical advantage in being so behind the technology times that crashing the entire global internet would leave it unscathed.

North Korea was also seen as unconstrained by alliances or friendships with other countries with more to lose in an Internet Armageddon.

"It could be anyone attacking anyone, but North Korea has an advantage," he said of his winning cyber battle plan.

"Some countries could already be in position. We can chose to limit our dependency on the Internet, which isn't realistic, or do our best to detect it and use politics to prevent it."

Miller took solace in the belief that some of the top computer experts needed to execute his plan would likely refuse to cooperate out of patriotism, morality, or plain fear.

"They might be scared you are going to kill them," Miller said. "It's a realistic thing to think about."

National Security Corporation president Mark Harding recalled graduating from officers school in the Navy having completed a thesis on how unprepared the country's military is for cyber war.

"There are people I know who have indicated they can take the entire Internet down and they can," Harding said.

"But, they don't because they believe in doing no damage and not taking anything that isn't theirs. It's when you lack a skill set of morality and

discipline when you end up on the dark side."

- PhysOrg.com [iPhone](#) / [iPad](#) Apps
- [PhysOrg.com Audio Podcasts](#) / [iTunes](#)
- PhysOrg.com [Android apps](#) (new version available)
- [Join PhysOrg.com on Facebook!](#)
- [Follow PhysOrg.com on Twitter!](#)

(c) 2010 AFP