U.S. and Russian experts turn up volume on cybersecurity alarms

Joseph Menn, Reuters

(Reuters) - Uncontrolled security threats on the Internet could return much of the planet to an era without electricity or automated transportation, top U.S. and Russian experts said on Thursday.

Former National Security Agency Director Michael Hayden warned that the United States had yet to resolve basic questions about how to police the Internet, let alone how to defend critical infrastructure such as electric generation plants.

And if recently discovered and government-sponsored intrusion software proliferates in the same way that viruses have in the past, "somewhere in 2020, maybe 2040, we'll get back to a romantic time - no power, no cars, no trains," said Eugene Kaspersky, chief executive officer of Moscow-based Kaspersky Lab, the largest privately held security vendor.

The back-to-back presentations at a Washington conference painted the starkest picture to date about the severity of the cybersecurity problem.

The past two years have seen an escalation of such warnings, especially about what U.S. officials have termed an unprecedented theft of trade secrets and. more lately, mounting threats to infrastructure.

At the same time, Congress failed last month to pass legislation aimed at protecting vital facilities, which Hayden bemoaned, and Kaspersky earlier this year detected extremely sophisticated surveillance programs that infiltrated personal computers and energy facilities in the Middle East.

If previous viruses were like bicycles, Kaspersky said, then the Stuxnet worm that damaged uranium enrichment centrifuges at the Natanz plant in Iran [1] two years ago would be a plane, and the latest programs, dubbed Flame and Gauss, would be "space shuttles."

Researchers are still dissecting those heavily encrypted viruses. Kaspersky and others say they are related to Stuxnet, which officials have privately admitted was designed by U.S. and Israel intelligence forces.

But Kaspersky said Stuxnet, Flame and Gauss would become templates.

Although Stuxnet infected thousands of machines in friendly nations, it was written by cautious "professionals" who minimized collateral damage, Kaspersky said at the Billington Cybersecurity Summit at the National Press Club. The knock-off versions by others will be much less discriminating, he added.

To show how quickly computer attacks can proliferate, Kaspersky said an electronic assault that disabled thousands of computers at Saudi Arabia's Aramco in mid-August had followed a separate infection reported by an Iranian oil company a few months ago.

Mounting a defense against nation-sponsored attacks will be extraordinarily difficult, Kaspersky said, as it requires new operating systems designed to manage equipment at crucial facilities. He said stopping criminals and terrorists who will adopt the same techniques would take strong international cooperation and deeper monitoring of the Internet, which many oppose on privacy grounds.

"We need to upgrade our understanding that the world is different," Kaspersky said. "We need to pay more attention to the critical information technology security issues."

Yet Kaspersky and Hayden said international treaties or even nonbinding agreements were nowhere in sight.

What is more, Hayden said, both the divided U.S. Congress and even different agencies within the executive branch have failed to reach a consensus on fundamental concepts, in part because the issues are still so new.

A Senate bill backed by President Barack Obama would have set voluntary cybersecurity standards for critical plants and allowed for greater information-sharing between intelligence agencies and private companies. But the bill encountered opposition from both the U.S. Chamber of Commerce, which objected to additional regulation, and the American Civil Liberties Union, which was worried about privacy issues.

The White House is now developing an executive order that would not go so far, but it still wants more powerful laws.

Even inside the administration, Hayden said, the Defense Department has defined cyberspace as a warfare domain that it must "dominate," while the Department of Homeland Security has publicly disagreed.

A core problem is that the same communications networks are used both for military operations and civilian transactions, which are protected from unreasonable searches.

While most Americans would welcome a local police officer shining a light at a shrub in their yard after seeing something suspicious, almost no one would feel the same way about questionable Internet activity.

The National Security Agency has the most advanced capabilities for cyberattacks and defense in the world, Hayden said.

"It is awesome," he said. "But nobody there has the authorization to defend you,"

because the NSA is generally barred from domestic eavesdropping.

As governments and companies recognize that they have all been hacked and focus more on limiting the damage from breaches, Hayden called for more extensive debate from civilians on how the United States should treat the Internet.

"You and I have not yet given our government guidance about what we want it to do," he said.

(Editing by Lisa Von Ahn)

Links:
[1] http://www.reuters.com/places/iran