By Jill Dougherty

On April 27, 2007, the tiny Baltic nation of Estonia - one of the most wired countries in the world - was hit with a massive cyberattack. Websites for banks, government ministries, newspapers, Parliament and media outlets were paralyzed, swamped by a distributed denial of service attack.

"We were frankly shocked when this happened," said Estonian President Toomas Hendrik Ilves. "Botnets attacked all aspects of society."

He contends it was "political act" in which Russia, angered over Estonia's decision to move a Soviet-era statue dedicated to a World War II Russian soldier in Tallinn, tried to shut down the country. Russia has always denied the charge.

But as bad as the attack on Estonia was, the next generation of cyberattacks could be much worse, Ilves said in a speech this month on "E-Governance and Cyber-Security" at Washington's Center for Strategic and International Studies. Distributed denial of service attacks are so "yesterday," he said. "... We can get around them."

Today, he warns, a new and more dangerous world of virus attacks threatens developed Western countries. "It's beginning to look ugly, and very ugly," he said.

These new viruses target the very DNA of modern life: SCADA (supervisory control and data acquisition) computer systems that monitor and control industrial processes, infrastructure like water purification, oil and gas pipelines, electrical power transmission, even supermarkets and cars.

"Our focus is too much on the military side of this," Ilves warns, "but, as someone once said, 'It's the economy, stupid.'"

Cyberattacks like these can be launched by countries as a form of warfare, with hired criminal gangs playing the role of armies carrying out the attack.

"It's not just students in dormitories in Beijing," Ilves said. "You can rent them and target someone."

The Estonian president says it's the intellectual property of Western countries that is being targeted, "the stuff that makes advanced Western societies function."

But the "bad guys" have an advantage over governments. In some countries there is no distinction between public and private. In others, the government utilizes what Ilves refers to as "public/private partnerships:" enlisting criminal cyber gangs in the service of the state.

In most Western countries there is a bright line separating public and private. "That Western model doesn't work anymore," Ilves stated, "and if it continues we're going to lose."

He believes it crucial for Western countries to "rethink" how they defend against that threat while, at the same time, maintaining that firewall. But most countries can't afford to hire all the people needed to do that. "All the geniuses in Silicon Valley" he said, "earn millions."

So, in addition to its own military and government information technology defenses, Estonia has created a "cyber National Guard" - approximately 100 volunteer "white-hatted hackers" he said - from start-ups and established IT businesses in the country who spend a certain amount of time, for free, protecting the country from cyberattacks.

"Making a lot of money becomes boring after a while," he laughed.

Cyberattacks are no laughing matter for NATO, which Estonia joined in 2004. NATO has a

cyberdefense research center in Tallinn.

Ilves said NATO needs to get moving on the threat. "It's flagging," he said. "Too many in NATO are in the 'so-what?' phase."

Cuts in defense spending are hurting, too, he says, and so is the "intelligence" model of dealing with threats.

"Cyberattacks will come from outside your borders and you need to cooperate with your allies," he said. Too often, however, NATO's members, as well as member nations of the European Union, he said, "don't talk with each other."

There's no time to lose, Ilves warned. "Cyberattacks will change dramatically our thinking about war and warfare."

Original article on the CNNäs Security Clearance webpage .