Aliya Sternstein

With a population smaller than that of Phoenix, the former Soviet republic of Estonia has grown skilled at taking down international criminal networks operating millions of computers, after the Internet-dependent society became the victim of one such ring in 2007. Now Estonia is sharing its cyber defense know-how with law enforcement agencies throughout NATO, including the FBI.

"Basically, your security agencies -- FBI -- are in fact establishing a representation unit, whatever you want to call it, in Estonia," Estonian President Toomas Hendrik Ilves said in an April interview with *Nextgov*.

FBI spokeswoman Jenny Shearer confirmed the relationship. "The Estonian National Criminal Police have consistently demonstrated their expertise and willingness to work as equal partners in the fight against cyber crime," she said.

Ilves was in Washington to meet with Army Gen. Keith Alexander, chief of U.S. Cyber Command -- another entity with which Ilves would like to partner.

The Baltic country has "a long-term, very deep and effective cooperation with the FBI on . . . [investigations into] stealing money, whether it's credit cards, through bank transfers," Ilves said. "We work very closely with them. They come to Estonia, we come here."

Estonia unintentionally became an expert at fighting computer intruders in 2007 when a cyberattack, reportedly sponsored by the Russian government, crippled the country's critical infrastructure and government networks for two weeks.

"The reason the cyberattacks had any effect is we had adopted in Estonia, we very consciously adopted computerization of society, government services, as our primary, fundamental motor of development," Ilves said.

While Estonia was under Communist control, the West was constructing highways, public transportation and modern facilities, "but when we came out of the Soviet [era] we were poor, the usual gray people living gray lives in gray buildings with falling-apart infrastructure or nonexistent infrastructure," said Ilves, 57. "We said building roads will take a long time, but we can, however, make a certain leap by computerizing as much as possible."

Today, officials estimate 98 percent of banking transactions are conducted online. While some U.S. precincts still struggle to count paper chads, Estonia has been voting on the Internet since 2005.

"That means you're very, very vulnerable because so much is online," said Ilves, who learned computer programming at age 14 from a math teacher in New Jersey, where Ilves grew up.

The intrusion that brought down Internet services in 2007 was primitive by today's standards, he said, pointing to malicious software such as Stuxnet, a sophisticated worm that reportedly derailed the industrial systems controlling Iran's nuclear operations by reprogramming the machinery to attack itself. In contrast, the distributed denial-of-service attack that hit Estonia was essentially a spam blitz coordinated by criminals funded, allegedly, by the Russian government.

"In general, what they do is all these computers that are robots, bot computers, are sending out all kinds of silly spam," Ilves said. "You can get all these networks of computers to send messages to one computer. Then you get hundreds of thousands of repeated messages to one address and you basically freeze out the server."

When Estonia's computer emergency response team deconstructed the incident afterward, a specialist showed Ilves that the onslaught reached its peak, "frizzed out everything" and then dropped back to zero. When the president asked why the barrage didn't slowly peter out after reaching its climax, Ilves was told, the money ran out. "I said, 'What do you mean the money ran out?' [The specialist] said these botnets were rented. There was probably a comparable

massive decline in the amount of Viagra spam. It was clear it was organized and paid for."

Such denial-of-service attacks are pinpricks compared to the amount of damage that adversaries now have the power to unleash with tactics such as advanced persistent threats, which lurk silently inside networks until they detect -- and download -- the intelligence they want. In March, just such a threat penetrated an RSA Security system containing information related to smart card IDs and key fob credentials used by many federal personnel.

"The amount of espionage that goes on, on the Web, is absurd and ridiculous," Ilves said. "I don't trust anything anymore."

He is particularly concerned about the vulnerability of the Internet phone provider Skype, a global business with research and development operations in Estonia. "They're putting millions [of dollars] if not more into developing new products and they have all these people working for them," Ilves said. "Now if someone gets into their system, takes out the new code that they've developed, they get it for free and they can start making exactly the same thing. This is what countries are waking up to finally."

Countries like the United States. In 2010, the FBI assigned a full-time cyber-trained investigator to work directly with the Estonian National Criminal Police on cyber crime matters.

"The FBI's decision to assign a full-time cyber investigator was based upon years of successful partnering on joint investigative matters," said Shearer.

Tallinn, the capital, is home to NATO's Cooperative Cyber Defense Center of Excellence, which is working to foster global cybersecurity collaboration by developing tools and best practices.

America could use some help in the cyber detective department, apparently. According to a re cent audit
by the Justice Department inspector general, more than a third of 36 FBI agents questioned said they lacked the networking and counterintelligence expertise to investigate national security intrusion cases.

Nevertheless, a joint U.S.-Estonia international investigation recently brought a major cyber ring to justice. In August, American law enforcement officials announced the extradition of a suspect from Estonia to the United States for arraignment on federal charges of, among other things, computer fraud and aggravated identity theft.

The Estonian suspect, aided by associates in Russia and Moldova, allegedly hacked into a network belonging to RBS WorldPay, the U.S. payment processing division of the Royal Bank of Scotland Group PLC, located in Atlanta.

Using customer data pinched from debit cards, the culprits in November 2008 generated 44 counterfeit cards to withdraw more than $9 million from ATMs in at least 280 cities worldwide, including cities in the United States, Estonia and Italy.

"Due to our strong partnership with the Estonian government on cyber matters, the case resulted in one of the first hackers extradited from Estonia to the United States," Gordon Snow, assistant director the FBI's cyber division, told lawmakers on April 12 at a hearing on cyber crime.

Original article on Nextgov homepage .