

by Rachelle G. Cohen

When the Soviet Union broke up in 1991, nearly all of its Central Asian "republics" retained their local dictators and even today remain at least politically frozen in time. But on the European side of the vast Soviet empire tiny Estonia grabbed for all of the freedoms it had been denied for five decades — and then some.

Today it is a member of NATO and the European Union, a world leader in use of the Internet (it's sometimes called Estonia) and an unwavering friend of the United States.

Its president, Toomas Hendrik Ilves, who grew up in New Jersey and has degrees from Columbia and the University of Pennsylvania, was among those who returned to the land his parents had fled when the Soviets invaded. And if he thought he owed a debt to the country that sheltered him during his formative years, he has been repaying it in full with some sage advice on cybersecurity.

"In today's warfare you don't have to attack a country with an army. You can wipe out a country's economy by attacking its banks," he told a forum last week at Tufts University's Fletcher School of Law and Diplomacy.

"You don't know where it's coming from and you don't know who's done it ... And because you don't have the forensics to figure out who did it — and you don't want to launch World War III by attacking the wrong guy," even fighting back is problematic.

He should know. Estonia, which has been ranked No. 1 in the world in Internet freedom for the past three years by Freedom House (beating out the U.S. and Germany, which came in second and third), was also the first nation to suffer a full-fledged politically motivated cyberattack on its government, banking and media sites back in April 2007.

But having put its voting online for the first time a month earlier, the nation had already built in the kind of redundancy needed to protect its systems. The government firewalls were not breached.

Still, Ilves insisted, "We are vulnerable in my country and you are vulnerable in your country.

"You may have the most advanced jet fighters in the world, but they are not much good if the lights go out."

And it is what we used to call "critical infrastructure," which is now all run by and off servers that remain vulnerable to cyberattack.

"You need to harden your systems and that's what we're faced with too," he added, noting that post-attack he put his "geek-in-chief" in charge of doing just that.

The alternative?

"Well, we could go back to 1989 — before iPhones and iPads and Internet banking and social media and Google. But I don't think we're willing to do that."

His largely student audience looked up from their iPhones long enough to laugh.

Fighting cybercrime also demands a concerted international effort by the world's "good guy" nations.

"The bad guys have a very robust private/public partnership," Ilves said, citing an astonishing and rather detailed mutual protection agreement between a ring of international credit card thieves and Russia's FLB, the successor to the old KGB.

"And there's a [Chinese] military base near Shanghai. A large part of the hacking that affects certain things come from computers all around that base — another public-private partnership," he added.

"Rule-of-law democracies have a firewall that prevents that kind of cooperation."

His is a rare kind of candor. Just as his nation's enduring friendship with our own is a rare kind of gift. Every conflict that has been fought — from Kosovo to Afghanistan to Iraq — Estonia has contributed troops. It even takes pride in paying its fair share of NATO's costs.

"People who lived under Communism for 50 years tend to appreciate their freedoms," he explains.

If part of his mission is to keep American isolationists from raising the drawbridge on fortress America, he did a helluva job. But then that's what you'd expect from a Jersey boy, isn't it.

Original article on the Boston Herald [webpage](#) .