*By Isabelle de Pommereau,
Correspondent, CSMonitor*

Ahead of spring elections, Agu Kivimagi was tasked with trying to ensure that online voting in Estonia wasn't vulnerable to attack. Its pioneering system of casting national ballots via the Internet would be a hacker's prize target.

After the ballots were counted, returning Estonia's center-right government to power, e-voting escaped assault - or any technical difficulties, for that matter.

Mr. Kivimagi, who oversees computer security for Estonia's Interior department, is part of the world's first volunteer cyberarmy, deployed this year to help ward off hacker strikes and defend against online warfare.

Made up of Estonia’s best information technology (IT) minds, from programmers to lawyers, the 150-member Cyber Defense League is Estonia’s cyber national guard. Should Estonia come under attack, they would deploy under the command of the National Defense League, a volunteer force created to safeguard the country's security and independence.

A reaction to Estonia experiencing a major cyberattack in 2007 - unofficially traced to Russian hackers - the volunteer cyberforce is an effort to get Estonians to participate in a societal, not just a military, task. Now, the tiny Baltic nation's e-defenses have captured the world's attention as hacker strikes grow in intensity - and the threat of cyberwar becomes increasingly real.

"We are only starting out, but I mention [the cyberarmy] initiative as the kind of solution that we need to begin to consider," Estonian President Toomas Hendrik Ilves said today at the 3rd International Conference on Cyber Conflict to Analyse the Nature of Cyber Forces, a gathering this week of more than 300 cyberdefense experts from 37 countries in Tallinn.

"We have slowly gotten to the point where we admit that cyberattacks and cyberwars are a major threat and not just child’s play by misguided hacker-geeks... . When threats are no longer classic threats, our response can no longer be classic either," he said, encouraging other countries to follow Estonia's lead in establishing all-volunteer cyberarmies.

NATO cyberpolicy

The 2007 attack also revealed NATO vulnerabilities. If Russian hackers could paralyze a whole country, what could a state-sponsored attack do? After the strike, Estonia lobbied NATO to establish a cyberdefense think tank in Tallinn and today NATO's Cooperative Cyber Defense Center of Excellence (CCDCE) shares space with a division of Estonia’s regular army.

In November, NATO made cybersecurity a strategic focus and stressed the need for greater cooperation among members of the alliance and international bodies, such as the European Union or the United Nation. And in Brussels today, NATO defense ministers adopted a new cyberdefense policy that clarifies political and operational mechanisms for an alliance response to cyberattacks. Under the new policy, all NATO structures will come under a centralized cyberdefense umbrella.

"Clearly, the policy makers in NATO have realized that cyberattacks are attacks, period, and that all the same rules apply as in other forms of warfare," Ilves told conference participants.

Attacks on the rise

Since 2007, cyberattacks have become fiercer and more frequent. Most attacks have been the work of what Mikko Hyppönen of F-Secure Corporation in Helsinki, calls "gangs of hackers."

But Stuxnet, the computer worm that successfully hit a nuclear reactor in Iran last summer, was the closest thing to an actual act of cyberwar. It appeared to be the first time a computer virus, which was so sophisticated that experts agree it could only have been backed by a government, struck a specific target in another state that was beyond the confines of the Internet.

"Stuxnet was the absolute game changer," says Mr. Hyppönen. "We are entering an arms race where countries start stocking weapons, only it isn’t planes and nuclear reactors they’re stocking but it’s cyberweapons."

"When it comes to cyberwar, it’s not a matter of if, it’s a matter of when," says Eneken Tikk, head of legal and policy affairs at the NATO cyberdefense center.

"It is becoming a trend. Technologically advanced countries have to count with the fact that politically sensitive decisions will result in cyberattacks," says Ms. Tikk. "We’re talking about cyber as a reaction base to whatever happens in society, using cyber means to send a message to governments."

A call for collaboration

One crucial part of the solution to many is additional public-private cooperation on cyberdefense.

"If the basis of our relative economic success, our private sector is coming under attack from state actors, we have to come up with new ways of talking to and sharing with the private sector,' said President Ilves. "This of course will run against the grain of how we have been doing things. Yet we need to address the problem."

Erik Laykin, a Los Angeles-based legal expert specializing in cybercrime, agreed and called for the US to start its own volunteer cyberarmy.

"Today, the battleground is your cell phone, your PC, your iPad, and this is why it is fundamentally a job of both the government and the citizens of a nation to develop a framework and response to cyberthreats," says Mr. Laykin. "Estonia is telling its people, 'You have a role to play in cyberdefense ... at stake is to protect your way of life, because a country's critical infrastructure is the fundamental that supports this way of life.'"

Since winning independence in 1991 again after 50 years of Soviet occupation, Estonia took to the Internet faster than its European neighbors. Embracing high-tech was a way to catch up to the West, says Linnar Viik, rector of the Estonia IT College in Tallinn.

"The Internet and IT infrastructure is a way of life, and this way of life and the values of this society aren't controlled by ministries of defense but are supported by culture, education, the economy," says Mr. Viik. "If the Internet stops working, society looses much of its functionality."

Original Article on The Christian Science Monitor homepage .