By Toomas Hendrik Ilves

Cyberwar is a new kind of threat, targetting infrastructure but also business, through piracy

In the past 20 years, Estonia has pioneered the use of Information and Communication Technology in government. ICT was the best, if not only way to leapfrog decades of backwardness resulting from Soviet occupation. Information technology and its use in the public as well as the private sector was the engine of our rapid development, enabling us to become a leader offering innovative solutions, which we gladly share with others.

Almost as if on cue, we also became the world's first victim of deliberate, directed, massive and across-the-board cyber-attacks – and, therefore, one of the world's centers of cyber-defense and security.

Five years ago, in April-May 2007, Estonian government sites, banks, newspapers, even the emergency number 112, were hit by so-called distributed denial of service attacks (DDOS), overloading servers. These attacks were politically motivated, yet they utilized criminal networks – botnets, the hijacked PCs of innocent users who had inadvertently downloaded malware.

The main use of botnets is spamming. Controlling malwareinfected computers is illegal everywhere, so botnets are run mostly by organized crime.

The cyber attacks against Estonia were not technologically unique – DDOS attacks had been used for years in economic crime – but it was a first in that it was political, a coordinated response to the Estonian government decision to move a statue of a Soviet "liberator" to a less disruptive place. Taking down government and private sector websites in a country highly reliant on Internet services was the continuation of policy by other means, which, as we know, is how von Clausewitz defined war. In a word, the cyber-attacks were a first in that they were directed at a country and they were ordered by someone, i.e. organized; they were political and thus ultimately, an act of war. Few if any wanted to admit this at the time.

Moore's Law, the empirical observation that the computing power of a chip doubles every 18 months, has a corollary in cyberconflict. Today's cyber-attacks are far more sophisticated than the decade-old use of DDOS attacks. Stuxnet-type worms can disrupt and destroy the ubiquitous Inter- and Intranet based control systems that run everything from our critical infrastructure to our cars and refrigerators. Industrial Control Systems (ICS) have made modern life far more comfortable and efficient, yet at the same time made us even more vulnerable.

Yet, I believe we concentrate far too much on the so-called hard security side of cyber. The real battles are ongoing and affect our security and well-being in altogether different ways than is generally discussed. Perhaps we are too fixated on militarization of cyber rather than state-sponsored theft. Slowly, the understanding is dawning that warfare need not always hit state or civilian infrastructure, but can also target our business sector, through piracy. In other words, in the immortal words of Bill Clinton: "It's the Economy, Stupid."

Espionage against states and increasingly against the private sector, especially areas dependent on R&D and intellectual property, is the other growth industry in an era of exponential computing growth. State and non-state actors including hackers and organized crime groups often work in a unique form of privatepublic partnerships to steal intellectual property that represents a company's hundreds of millions of euros and years-long research and development.

Let's face it: our companies are coming under massive attack. This is true everywhere in the West, where intellectual property is a key component of our national wealth. It may be difficult to steal a country's oil or its agricultural or even manufacturing wealth, but given the billions, as well as years invested in intellectual property, it can be all stolen in a matter of minutes or a weekend. This is industrial-strength piracy and a genuine security threat, not just a worry of Hollywood film companies.

For technologically advanced countries, including my own, with Tallinn as the R&D center of our flagship company Skype, it is the theft of intellectual property that can in fact cripple or at least severely wound our economies. Let's be sure about this: much of what makes modern economies function and prosper is the product of huge R&D investments, both public and private.

The EU has set a goal for its member states to invest 3 percent of GDP in R&D, a goal few meet (but then again few meet the NATO goal of defense expenditure of 2 percent of GDP).

Much of the democratic West's primacy rests on innovation, on new designs, pharmaceutical products, software solutions etc.

A company that invests hundreds of millions or even billions of dollars or euros in new products can see it all evaporate if the research is stolen: the value of the product comes from those years of creative work and money invested in developing it. Yet it can all be stolen. At which point someone else somewhere else has gotten for free what your country's best and brightest spent years to develop. You lose the tax revenue, someone else reaps the profits.

This is piracy. Pure and simple. And it is as dangerous and threatening for modern states as piracy in its more primitive forms off the Barbary Coast was at the beginning of the 19th Century or in fact today off the coast of Somalia. As is the case with classical marine piracy, intellectual property piracy is not only a threat to our economies, it is also a threat that falls into the category of PPP or public-private partnership, where state actors condone or turn a blind eye to it, if it benefits their economies, or even explicitly make use it as the Barbary States did under Ottoman rule. And as with the Barbary pirates, cyber-attacks against our companies can be met head on only with cooperative and concerted state action.

Proceeding from this, the major concerns we have to deal with include: paralysis or destruction of critical infrastructure that today is largely computer-run; espionage, against both governments and the private sector; lack of public trust in electronic databases; lack of allinclusive databases. This in turn means we must take a multi-track approach: defense of critical infrastructure is a task for governments and NATO, defense of the private sector requires a rethink of government and private sector relations.

In Spring 2008, NATO established its Cooperative Cyber Defense Center of Excellence in Tallinn, serving as a valuable source of expertise in the field of cyber-defense for both its sponsoring nations and NATO. Its interdisciplinary approach to cyber-defense is what makes the Center unique: experts from different fields work together and share their knowledge, giving the Center and its work a broader perspective. The Center aims to become the main source of expertise in cyberdefense by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners.

At the end of this year, the Center will publish a National Cyber Security Framework Manual meant to support allies and partners as guidance to develop, improve or confirm their national policies, laws and regulations, decision-making processes and other aspects of national cyber-defense. The target audience will be all stakeholders of national cyber-defense including leaders, legislators, regulators and service providers.

In addition, the Center also offers opportunities to train specialists to deal with potential cyber-attack through the Live Fire Cyber Defense Exercises, such as the annual Locked Shields exercise. The goal is to involve as many participants as possible so that specialists of different countries can practice in real terms what it feels like to cooperate at times of crisis.

The Center also aims to give more support to NATO exercises, such as the annual Cyber Coalition and to the 2012 NATO Crisis Management Exercise. Ideally, cyber should become an integrated component to every NATO exercise.

We will have to rethink government-private sector relations. While Freedom House ranks Estonia as number one in the world in Internet freedom (followed by the United States and Germany), we need to ensure that the freedom is secure from those who would abuse it. Yet if the basis of our relative economic success, our private sector, is coming under attack from state actors, we need to come up with new ways of talking to, and sharing with, the private sector. This of course runs against the grain of how we have often been doing things. Yet we need to address the problem. As I see it, there are two issues.

Firstly, we need to come up with new ways to talk to the private sector. Security clearances, sharing of sensitive information – in both directions from government to private sector and vice versa needs to be made far less ad hoc, far more based on rules that would allow us a greater deal of flexibility to face new threats without at the same time allowing the crony capitalism that destroys democracies.

Secondly, however, we on the state-side of things need the brains that go to the private side of ICT. Let's be honest, Estonia can't pay for the genius software developer at Skype. But then again, the US Department of Defense most likely is not able to hire the top guns at Apple, Microsoft or Google either. The other side(s) can. Back during the Manhattan Project, the US could hire Edward Teller or Robert Oppenheimer for a professor's salary. But nuclear physicists

could only work for a university or for the government. Today neither the university nor the government can afford the modern cyber equivalents of an Edward Teller.

All this puts governments at a disadvantage in developing cyber defense. We cannot necessarily afford the best and the brightest. Here in Estonia, however, we have developed one solution to this problem, the Cyber-Defense League, which we can translate, depending on your own national version as the Cyber Home Guard or the Cyber National Guard. These are weekend warriors with ponytails, computer geeks who have high-paying day jobs running IT departments, working in software companies, banks etc., who find it cool to volunteer for their country. We offer them the opportunity to help with our defense. Not running around the woods in camouflage suits but building our cyber-defense capability. They are motivated and patriotic, and let's be honest, it's sexy to work on these things.

I mention this initiative as the kind of creative solution that we need to begin to consider to be able to guarantee the highly sophisticated e-services and the high R&D driven companies a modern society depends upon. When threats are no longer classic threats, our responses can no longer be classic either – at least if we want to maintain the upper hand.

This means that we need to give new impetus to the otherwise shop-worn concept of co-operation. Governments and states need to get out of the intelligence paradigm where nothing is shared with allies, to a paradigm of interoperability and common response. The private sector and the state need to negotiate new forms of co-operation that will initially be uncomfortable for both but which are the sine qua non of maintaining our economic well-being.

Estonia's experience in the past 20 years reflects this: we are e-believers. We are proud of being pioneers in e-government. And we are convinced that a public sector ICT approach that is citizen-centered, secure and transparent is the future of good governance in the 21st century.

Original article on the Security Times webpage .