Cybersecurity: A View From the Front

PROPOSITION

Toomas Hendrik Ilves, President of the Republic of Estonia

The changes in the digital world today represent a dramatically sped-up version of the changes the world underwent in a century of industrialization. It is a paradigm transformation of our world: notions of a nation's size, wealth, power, military might, population and GDP mean something altogether different from what they meant a generation ago.

Toomas Hendrik Ilves is President of the Republic of Estonia. Ilves served a.o. as the Ambassador in Washington and as Minister of Foreign Affairs. He is currently Chairman of the European Cloud Partnership Steering Board and has written extensively on European integration, transatlantic relations, e-government and cyber security. Ilves holds a Master's degree in Psychology from the University of Pennsylvania.

These relations are in constant flux, and old assumptions no longer hold. Today, a small, poor East European country can be a world leader in e-governance and cybersecurity.

In February, the United Nations praised Estonia's e-Annual Report system, by which entrepreneurs can submit annual reports electronically, as the "best of the best" e-Government application of the past decade. Last autumn, Freedom House ranked Estonia first in Internet freedom for the third year in a row (the United States and Germany were second and third).

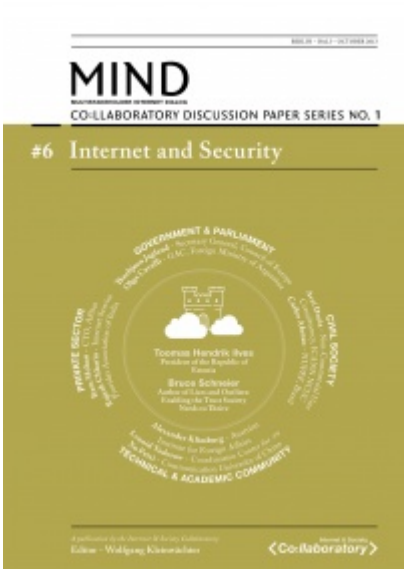
At the same time, Estonia is also remembered as the first publicly known target of politically motivated cyberattacks in April 2007, which inundated the websites of Parliament, banks, ministries, television stations and other organizations.

Disruptive as the attacks were, they were by today's standards primitive, consisting of "distributed denial of service" attacks (DDoS), which essentially overload servers with signals from hijacked, hacker-controlled PCs. Six years later, as computing power and IT dependency have increased hugely, cyberattacks are far more sophisticated and our vulnerabilities are far greater.

Yet those attacks were a blessing – Estonia took cybersecurity seriously earlier than most. In 2008, NATO opened its Cooperative Cyber Defense Center of Excellence, to enhance NATO's cyberdefense capability, in Tallinn.

Cybersecurity needs to be taken seriously by everyone. We continue to think of cyberthreats in military or classical warfare terms, when in fact cyber can simply render the military paradigm irrelevant. The whole information and communication technologies (ICT) infrastructure must be regarded as an "ecosystem" in which everything is interconnected. It functions as a whole; it must be defended as a whole.

MIND #6
Table of Contents
PDF Download



Today, almost everything we do depends on a digitized system of one kind or another. Our critical infrastructure – our electrical, water or energy production systems and traffic management – essentially interacts with, and cannot be separated from, our critical information infrastructure: private Internet providers, lines of telecommunications and the Supervisory Control and Data Acquisition (Scada) systems that run everything from nuclear power plants to delivery of milk to our supermarkets.

Understanding that cybersecurity means defending the entirety of our societies, we need to re-examine many assumptions of security. In cyberwarfare, it is much harder to identify the attacker, and therefore to know how to retaliate.

In a modern digitized world it is possible to paralyze a country without attacking its defense forces: the country can be ruined by simply bringing its Scada systems to a halt. To impoverish a country one can erase its banking records. The most sophisticated military technology can be rendered irrelevant. In cyberspace, no country is an island.

This requires rethinking some of our core philosophical notions of modern society: the relations between the public and private spheres, between privacy and identity.

At a time when the greatest threats to our privacy and the security of our data come from criminal hackers and foreign countries (often working together), we remain fixed on the idea that Big Brother, our own government, is the danger.

This may have been true in the past, when only national governments had the ability to monitor citizens. Today, as we know, a single hacker can access the most intimate details of your digital and nondigital life, your finances and your correspondence.

This is a clear case of market failure. A bank that builds identity theft and fraud into the cost of doing business is an example of market failure. A power company that treats a cyber-induced power outage as an act of God, no different from a tornado or earthquake, demonstrates market failure.

If the private sector is unwilling to take the necessary steps to guarantee the integrity of its online activities, the government must step in to fulfill its most fundamental task – to ensure the security of its citizens; that is, to provide them with a secure identity.

Identity lies at the core of security online. Virtually all breaches of computer security involve a fake identity, be it stealing a credit card number or accessing the internal documents of the European Commission. A three-digit security code on the back of a credit card does not provide you with a secure identity, nor does an ordinary computer password. The fundamental question is whether you can be sure the person you interact with online is who he claims he is.

The key to all online security is a secure online identification system. But a nebulous fear of an imagined Big Brother prevents citizens in many places from adopting a smart-chip-based access key that would afford them secure online transactions.

In Estonia, the government has become the guarantor of secure transactions online, while identity is authenticated by a body independent of the government. We use a two-factor identification system in which the ID is protected by both a chip and a password. A binary key or public key infrastructure guarantees securely encrypted transfer of information. Thus far, our system has proved secure. Even during the DDoS attacks of 2007, our digital government system remained online and intact.

Precisely because we offer a verifiable and reliable identification system, Estonia has gone further than any other country in investing in digitizing the basic processes of society. A quarter of the electorate votes online, 95 percent of tax returns are done online and 95 percent of prescriptions are filled online. By the end of 2012, Estonians had given more than a hundred million digital legal signatures. Citizens, as legal owners of their own data, have access to their digital medical and dental records. And we have more and more e-services available every year.

In the future, we hope to connect our digital services and make them interoperable with our neighbors in Northern Europe. In the longer run, we're looking toward uniting systems in all of Europe. Ultimately, government data will move across borders as freely as e-mail and Facebook and follow the international flows of commerce and trade.

The job of cybersecurity is to enable a globalized economy based on the free movement of people, goods, services, capital and ideas. This can only be accomplished if identities are secure.

Undoubtedly the most effective means by which our societies could be safeguarded from cyberattacks would be to roll back the clock – to go back to the pen, typewriter, paper and mechanical switch. We should give up on mobile phones, iPads, online banking, social media, Google searches – everything we have become accustomed to in the modern world. But that won't happen.

Cybersecurity is not just a matter of blocking bad things a cyberattack can do; it is protecting all the good things that cyberinsecurity can prevent us from doing. Genuine cybersecurity should not be seen as an additional cost, but as an enabler, guarding our entire digital way of life.

MIND-Multistakeholder Internet Dialog
MIND stands for Multistakeholder Internet Dialogue. The discussion paper series is a platform for modern polemics in the field of internet governance. Each issue is structured around a central argument in form of a proposition of a well-known author, which is then commented by several actors from academia and the technical communities, the private sector, as well as civil society and government in form of replications. **all MIND-publications**