At a time when cyber warfare is acknowledged as a real threat and nations like the US resolve to treat attacks on its computer networks as an act of war requiring a military response, Estonian President Toomas Hendrik Ilves talks about the crippling spate of cyber attacks that hit his country in the spring of 2007.

Boasting one of the world's highest levels of internet penetration, Estonia was especially vulnerable to the series of crippling cyber attacks launched from Russia in the spring of 2007; attacks attributed to Russian outrage over the removal of a Soviet war memorial from the centre of Tallinn, the Estonian capital.

After 50 years of stagnation under Soviet occupation, Ilves had proudly noted, “there was no need to be slow on the IT side of things and very quickly (Estonia) became one of the most computerised countries in Europe.” Today, Estonians rely almost exclusively on the internet to access government services, file their taxes and conduct bank transactions. Free Wi-Fi reaches nearly every corner of the small country.

What first caught Estonian authorities' attention was that the attacks, which began on 27 April and lasted until mid-May 2007, did not follow the usual pattern seen in previous distributed denial of service (DDOS) attacks, whereby the attack ramps up to a peak and then falls off over time. This time, Ilves said, a new, more troubling pattern emerged.

Asked to give an example, he cited one particular attack that began precisely at 00:00 Moscow time 9 May at “an incomprehensibly high level” and ceased completely exactly 24 hours later. The attack began and ended according to the strict terms of a contract between a criminal organisation and an unknown party – precisely one full day of attacks on selected Estonian government websites. It was later determined that the botnets attacking Estonia were controlled by a known Russian criminal organisation.

In sum, Ilves said, the attacks were a “hitherto unseen form of public-private partnership.” In fact, he continued, “if you accept that this is warfare then it is a new type of warfare; criminal gangs were used to attack the critical infrastructure of a nation state.”

While Estonia had issued warnings within NATO about attacks against national infrastructure, the 2007 assault served as a wake-up call. Coincidentally, just months before the attacks, the alliance had opened the Cooperative Cyber Defense Centre of Excellence in Tallinn to grapple with the theoretical and legal issues surrounding cyber assault and defence.

What should NATO do if a country falls prey to cyber attackers?

Of all the problems the centre seeks to solve, Ilves said, the thorniest is whether or not the NATO Treaty's Article 5, stipulating that an attack against one member is an attack against all to be met with a proportional response, applies in the event of a cyber attack. "What do you do in the case of a cyber attack where you don't know who did it? You could have a guess and there is probably a correlation in time with political developments but (at the same time) they could be false flags. And then you must decide what constitutes a proportional response."

"It's not that you can't determine who carried out the cyber attack, it just takes a long time. It's more similar to the forensics done in the wake of terrorist attack when no group claims responsibility or, as is often the case, when many different groups claim responsibility."

Defining the threat is another challenge, Ilves noted. "What is a cyber attack? What is cyber crime? The hackers that are stealing money are also developing software to break into government systems." Yet, "at the same time, I would argue that our boundaries are too strict."

Conventional wisdom has divided cyber concerns into two defined, unrelated realms - those of the government (Pentagon, State Department, etc) and those of the private sector (e-commerce, personal email). In fact, Ilves said, there is considerable overlap.

European leaders addressed the danger cyber crime poses to their national economies for the first time this past February at the Munich Security Conference. Discussion topics included the realisation that “one of the biggest threats to national security is intellectual property theft,” Ilves noted. Years of work and billions of dollars in research can be lost in mere seconds through a cyber attack. The high-tech and pharmaceutical sectors are especially vulnerable. If such corporations are crippled or even driven out of business through cyber theft, the tax base is lowered and the whole country suffers, he explained.

The culture of secrecy related to IT security has prevented effective work in the past because “cyber” is one of the most national of defence issues, Ilves explained. While NATO requires the use of interoperable military equipment and weapons its members have carefully guarded their IT systems from each other as much as from enemy forces. “We also see this in the European Union although this has begun to change over the last few years.”

Co-operation between NATO and the European Union “has not gotten to where it should be” despite the huge overlaps in their membership. Much of the blame, Ilves said, lies at the feet of bilateral issues. “As long as we have one EU member blocking co-operation with NATO and one NATO member blocking co-operation with the EU, we don't have the necessary security co-operation. If there is one area where we could really use it, it is in the area of cyber security and cyber defence.”

Making cyber defence more of a public issue than it has been up until now is critical. “Bad guys are doing public-private partnerships. What we need is the good guys doing the same.”

“The firewalls between the government and the private sector, put in place for good reason, may in fact have become a liability. This is something we need to think about more,” Ilves advised. To fight back, “we need to create our own public-private partnerships with the IT sector” because they face a common threat. As one high-tech corporate head told him recently, “when governments are not being attacked, we are.”

Estonia has pioneered the concept of recruiting private citizens to volunteer their time to protect their country's critical IT infrastructure. At the beginning of this year, Estonia's Cyber Defense League, the world's first all-voluntary cyber national guard, was announced. Ilves proudly referred to the force of private and public sector IT pros as a “white-hatted hacker corps.” Unsurprisingly, the concept has generated great interest from other European countries.

He explained further: “If you have such an IT-dependent economy, then your country is full of people who work in corporate IT departments. They're developing new things and they like their jobs but it's not necessarily that cool. What we have said to them is, 'in your spare time, come and develop stuff to defend your country.'” The response has been overwhelming.

“What we really need to do is develop a system of conventions” on cyber warfare, Ilves suggested. The Council of Europe concluded the one existent treaty more than a decade ago. That pact holds that if entities in a country are found to be involved in cyber crimes then the government of that country is responsible for conducting a criminal investigation. The list of signatories includes most of the world’s democracies but, critically, not Russia, despite Moscow's membership in the Council of Europe.

It is on this rock that cyber security treaties and conventions have foundered. Since attacks are carried out through botnets scattered all over the globe, the attack itself rarely, if ever, will emanate from the attacker's home country. Furthermore, the use of private criminal entities to set up and launch the attack provides a significant degree of deniability for the instigating government. Therefore, Ilves fretted, it is highly unlikely that blame can be ascribed with a degree of certainty sufficient to trigger a collective military response and certainly not within sufficient time for the gun to still be smoking, as it were.

The future of cyber warfare

In February 2010, Russia released its latest 'Military Doctrine', which referenced cyber warfare. Ilves, however, is not as troubled by this since Moscow is “stating a reality that exists.” It is Russia's refusal “to sign up to fundamental rule of law (and) liberal democratic ideasÂ in the Council of Europe Convention,” however, that is “more worrisome than blustering statements and doctrines.”

Non-democratic countries “seem to have a real need to control the internet” which, paradoxically, Ilves said, makes it harder for them to deny knowledge of cyber crimes emanating from their territories. A law passed in the Duma in 2003 requires that all Russian ISPs route their traffic through the FSB, the successor to the KGB intelligence service. “That makes Russia’s lack of co-operation even more strange.”

“Cyber crime is by definition extra-territorial,” Ilves stated. Countries have different understandings of national security and so co-operation tends to be bilateral and issue-oriented. Some are quite reticent to share and others much more open to co-operation. “We have, for example, amazingly good co-operation between the FBI and the Estonian security services. In fact, the FBI and various other institutions are about to set up an office in Estonia because our 'cyber cops' have been instrumental in covering all kinds of stuff that has happened in the United States originating from various places in Eastern Europe,” he said.

Estonian President Toomas Hendrik Ilves recently flew into Washington for brief working visit devoted to cyber security. He met with Gen Keith B Alexander, Commander of the U.S. Cyber Command, and spoke with Journal of International Security Affairs *deputy editor James Colbert*

Original article on the Silicon Republic homepage .