

Cybersecurity: Keeping Europe Safe and Free in the 21st Century

Address by Dr. Mart Laar (Minister of Defence, Republic of Estonia) to the European Security Roundtable on 14.06.2011

January: The EU's Carbon Emissions Trading Scheme goes offline after more than €28 million in permits were stolen through cyber attacks.

February: an ex-official tells reporters the UK Ministry of Defence suffers 600,000 automated botnet attacks per day.

March: EU Commission servers comes under a large-scale attack, probably to steal sensitive documents for the EU summit in Hungary.

April: Cyber-criminals steal the personal and credit card data of 100 million Sony Playstation users

May: Lockheed Martin announces it has stopped a major cyber attack. Earlier cyber attacks on the company may have stolen data on the F-35, a jet fighter many European countries are buying.

June: The IMF suffered a targeted cyber attack that gave one country a digital insider presence in the fund. More humorously, a 16 year old girl named Tessa accidentally invites every Facebook user in Hamburg to her birthday party, and 1,500 people to swarm her quite home street.

All of these events follow 2010, when we learned that a virus named Stuxnet took over and ruined Iran's uranium centrifuges. There were no casualties, but the same attack could be used to explode power plants, poison water supplies and derail trains. 20 years ago, we hoped the end of the cold war would mark an era of peace. Today, we know that we are under ever more constant attack... under cyber attack!

Ladies and Gentlemen, Welcome to the cyber age!

The explosive growth in the internet has already transformed the world, connected over 2 billion users, started new industries and sparked revolutions. Today's 2 billion netizens are being joined by another 2 billion connecting to the internet through smart phones and mobile devices, mostly in the developing world. As we speak, an "internet of things" is also coming into existence – the chips in your car, clock, and toaster oven are all joining the web. Today's tools let us create, analyze and organize this information to create more knowledge at a lower cost. If knowledge is power, there is a lot more power flowing about today. Much of that power has gone to good use, from sequencing the genome to analyzing markets to spreading democracy.

The internet is a tool of freedom. Information brought down the communist system. Today, the internet has sped up the free movement of information and exchange of opinions. The internet is bringing down totalitarian governments around the world and is now the most feared enemy of every dictatorship. In attempt to deny freedom for their people, modern dictatorships are trying to block internet access, build walls against the movement of information, punish netizens and criminalize the free exchange of ideas.

But even more dangerous are the attacks they launch on the internet in free countries, trying to make it impossible for us to use of one of our main rights – freedom. Make no mistake –cyber wars are an attack against our way of life and principles, and on the basis

of our knowledge-based economies. Freedom, achieved via modern technology, is one of the greatest achievements of modern society – giving it away means catastrophe and ruin for us all.

The Internet was built by good guys, who could not imagine the open architecture they were creating would also empower bad guys: anarchists, petty criminals, fraudsters, organized crime, terrorists, rogue states, dictatorships – the internet and knowledge help them do what they do best, only faster, cheaper and easier. Just a few years ago, cyber defence and security were fringe issues, fit for nerds and geeks. Estonia has been a bit of an exception: we experienced massive cyberattacks in 2007 against our banks, government and media. These attacks were part of a larger, coordinated strategy to disrupt our e-lifestyle and internet way of life and destabilize our government. We defeated the attacks, but also realized how vulnerable our modern societies are.

We learned three truths from this first cyberwar, which have since been repeated time and again in ever more dangerous cyber attacks: First, break down boundaries: the old dividing lines between defense and security problems, law enforcement and military solutions, public and private don't hold in cyberspace. No single ministry or department can handle what is simultaneously a problem of infrastructure, defense, law enforcement, commerce, and civil liberties. Government needs to coordinate activities across ministries, using broad national cyber-security strategies and appointing lead individuals or agencies. The same measures that protect us against cyber-crime and hacktivists will also help protect us against cyber-terrorism and strategic attacks on the whole of a country.

Furthermore, 85% of web infrastructure is in private hands. 80% of cyber-attacks are launched against private companies, NGOs, and individuals. Critical civilian infrastructure depends on the private sector for security, even when owned by the state. Force and regulation alone won't work: the private sector needs to want to work with government, so incentives and cooperation must be well-designed.

Second, practice good cyber-citizenship. To secure cyberspace, every owner of a computer, computer network or information system needs to feel responsible for the proper and prudent use of computers and web technology. Washing our hands and food prevents viruses and bacteria from spreading. Similarly, cyber hygiene prevents computer viruses and attacks from spreading. Good cyber hygiene comes through both regulation and awareness campaigns. 80% of cyber attacks can be prevented through simple steps like updating Virus software and downloading responsibly. Consider: if computer users in the US and Canada had employed better cyber-hygiene, many of the attacks against Estonia in 2007 simply would not have occurred. Had Estonia itself used better cyber hygiene, many of the cyber attacks against Georgia in 2008 would not have occurred.

Citizens can also participate more actively in cyber-defence. Estonia found an innovative solution to the difficulties of finding qualified cybersecurity manpower by creating a cyber division to our all-volunteer home guard. Our best cybersecurity experts from the private sector and academia have joined the Cyber Defence League, and form a volunteer pool of IT specialists, programmers, and hackers. Should we face another massive strategic cyber attack, they will help keep us safe.

Third, deepen international cooperation. There are no border controls or Schengen agreements in cyberspace. The bad guys operate without regard for geography. So should we, by exchanging information and analysis about attacks, harmonizing legal definitions, setting standards for security, fostering informal cooperation, supporting joint research and

development, assisting each other in case of attack, and modernizing collective defence and humanitarian law for cyber conflicts.

International cooperation requires countries to become good global cyber-citizens. Today, quite a few countries are safe havens for illegal cyber-activity. Cyber crime is bad in and of itself, but it also supports other forms of organized crime, terrorism, and state sponsored attacks. Countries outside of Europe need to join the Council of Europe's Convention on Cyber Crime. In addition to mandating cooperation, the Budapest Convention also sets standards for domestic legislation. The willingness of third countries to join this treaty is good proof of whether they have the good will to tackle cyber crime. The US has signed the convention, but Russia (a member of the Council of Europe) and China have not.

Today, cybersecurity has become a mainstream issue. Many countries have now produced in-depth strategies and policies for tackling risks from cyberspace. NATO just approved a new cyber defence policy.

Unfortunately, recognizing the problem is not enough: the gap between our ambitions and our actions is fairly large. Despite the need for cooperation, there are still trust issues: intelligence people don't want to share sensitive information for national security reasons, companies for competitive reasons; government doesn't trust individual hackers and civil society, and individual hackers and civil society don't trust government. And so on. We also need large new investments, but face resource constraints and austerity measures.

For these reasons, it is clear that the EU is important to our hopes for increasing global cyber-security. The EU has resources, expertise, and competence. Many problems in European cyberspace – like protecting critical infrastructure, fully harmonizing law enforcement, or deepening cooperation between CERTs – can only occur on an EU level. The EU's diplomacy and missions are a key part of making international cyberspace safe.

With this in mind, I offer some practical proposals:

1. Coordinate Europe's current activities

We need to start with ensuring national and EU institutions' networks are secure and have not been penetrated. The EU needs to fully audit its systems to prevent the types of targeted attacks I mentioned at the beginning of my talk. Otherwise, we face not a nebulous future threat, but a clear and present danger to our security.

While the EU already does much to ensure cyber-security, many of these activities are quite fractured, split across directorates and agencies. The EU needs to better coordinate its own cybersecurity activities through an ambitious agenda. Europe also needs better coordination with Member States. There are few EU guidelines or recommendations on what countries should be doing to secure their cyberspace, which has led to a growing gap between member states in the effectiveness and breadth of cyber security measures and cooperation. One vulnerable Member State leaves the entire Union open to attack.

The EU should focus on areas where it is particularly competent. These include protecting critical infrastructure, coordinating legal structures, regulating and working with business, consumer protection and privacy, anti-terrorism.

2. CFSP: Cyber in the center of Europe's diplomatic agenda

Cybersecurity needs to be a part of every EU diplomatic relationship. We need to use the Common Foreign and Security Policy to extend Europe's cyber-security agenda across the globe.

The EU is currently holding talks with the US on a wide range of these issues, including reacting to incidents and attacks, encouraging public private partnerships, raising awareness and fighting cybercrime. Unfortunately, these talks are going slowly, when we should be broadening them to other allies.

We should target our development aid to encourage good cybersecurity in developing countries, where we need to stress that cyber-security is compatible with individual rights, privacy and free speech. We should apply diplomatic and economic pressure on countries that won't cooperate internationally on cybercrime or harbor cyber-criminals and terrorists.

These steps need a stronger External Action Service. The EEAS has so far not filled its few positions for cybersecurity experts, when it needs a dedicated branch and sizeable corps of experts coordinating Europe's international engagement. Because of a lack of manpower, there are important ongoing global discussions - developing norms of behavior in cyberspace, new forms of internet governance, confidence building measures in the OSCE – where the EU is not participating.

3. Cyber-CSDP

As a minister of defence, I look in particular to our Common Security and Defence Policy. Incredibly, cyber defence is not currently built into the CSDP's missions or activities, even though the CSDP's hallmark, a joint civil-military approach to security, is particularly well-suited to cyber defence problems.

First, the CSDP must ensure that forces on EU military and humanitarian missions are protected against cyber attacks. Otherwise, we might see expensive, politically fragile large missions derailed by inexpensive exploits costing a few dollars. We hope to use the EU's Nordic Battle Group as a pilot for such capabilities.

We must then go further, and make cyber defence an active capability of the CSDP. Just as we deploy civilian forces to develop local institutions, law enforcement and border security, provide aid and prevent conflict, we should deploy EU Cyberdefence Teams. These teams could react quickly to cyber attacks or crises, and would help build up national cyber defence systems, test for vulnerabilities, develop legislation and reforms, and encourage cooperation with experts in the EU. They would also be useful in reacting to cyber emergencies within the EU.

NATO is developing some of these capabilities, but not all. It is crucial we coordinate EU-NATO activities in this area – there are many overlaps and win-win solutions, but we aren't taking advantage of them today.

.....
Ladies and gentlemen,

Estonia's commitment to Europe's cybersecurity is enduring. We see this issue as a way for us to make an outsize contribution to our common security. Tallinn is quickly becoming a hub for cybersecurity. We currently host NATO's Cooperative Cyber Defence Center of Excellence, which is also a useful nexus for EU-NATO cooperation. The NATO center will soon be joined by the EU's Schengen IT agency. We also operate one of the few advanced degree programs in cybersecurity, and are home to many innovative enterprises in the field.

Estonia can not be a lone voice in the desert. Every day that Europe does not act, we all suffer attacks on our freedoms, put our publics at grave risk, undermine the security on which a common European space is built, and suffer billions of Euros of damage to our economies and intellectual property. If we were suffering this damage through bombs and bullets, our citizens would be up in arms. But make no mistake, the threat from cyberspace is just as real and tangible. Defending ourselves against cyber attacks is perhaps Europe's seminal security challenge in the early 21st century. I truly hope today and tomorrow's discussions spark important and urgent action. With that in mind, it is time to put on our thinking caps and roll up our sleeves. Thank you!

UK, Estonia, Denmark Joint Statement

Joint Statement by Dr. Liam Fox, UK Minister of Defence, Gitte Lillelund Bech, Danish Minister of Defence and Mart Laar, Estonian Minister of Defence after their meeting in Kabul on 16/06/2011.

We are on the eve of the 5th anniversary of our joint mission in Southern Afghanistan. Over these five years the United Kingdom, Denmark and Estonia have worked side-by-side, adopting a comprehensive approach in our mission to make excellent progress in the region. Together, under the auspices of Task Force Helmand, and with the Afghan authorities and security forces, and other NATO allies - particularly the US - we have achieved significant results in improving the security in an area previously renowned as a Taliban stronghold. We remain committed to the ISAF campaign.

We continue to build upon these gains in order to ensure irreversible progress through developing the Afghan National Security Forces (ANSF), who have an essential role to play in providing both security and governance in Afghanistan. Building the capacity and capability of the ANSF will increasingly allow Afghanistan to take responsibility for her own long-term security and stability. As the NATO Secretary General said "Trainers are the Ticket to Transition". We remain committed to supporting the NATO Training Mission Afghanistan (NTM-A) led ANSF training mission and to wider capacity building in Afghanistan and will continue to support this effort through the Helmand Provincial Reconstruction Team.

These development efforts are paying dividends. We welcome the inclusion of Lashkar Gah in the first tranche of transition areas, in which we will continue to transfer lead security responsibility from ISAF to the ANSF this summer. The ANSF will be in the lead of security provision by the end of 2014 and though the nature of our forces might evolve during the Transition process, we must ensure that the mission is appropriately resourced, and a balance maintained between combat troops (to prepare the ground to allow the rest of central Helmand to enter Transition) and trainers (to further develop the ANSF). Transition will free up troops; members of ISAF who, due to transition in their areas, will be relieved from their combat tasks are encouraged to find ways to contribute their troops to regions where stability operations continue or find other means of engagement.

All three of our nations have a long term commitment to Afghanistan and, together as part of NATO, we are pressing ahead with planning how this will evolve through and beyond transition.