Cyber-security and liberal democracies

For the last three conferences here in Tallinn, I have focused on technological threats from cyberspace. I shan't spend much time on these matters today. Recent events only have confirmed and brought into the public eye what you at this conference have been discussing for years.

What has changed, though, is the overall level of international awareness of cyber threats. Five years ago, Estonia was a lone voice in the desert raising the alarm. Cyber defence now is the hottest topic in Washington, London, Paris and many other capitals, though I regret that there is a paucity of strategic awareness about this in Brussels. This year, there was a long waiting list to get into this conference. Next year, we shall probably need a bigger venue.

Cyber is everywhere, permeates everything

Today, however, I don't want to talk about cyber defence. Defence is only sensible with regards to an object to be defended, so I want to ask – what is it that we are defending when we speak of cyber defence?

Cyberspace is quickly growing to encompass the whole world. You know the indicators: two billion netizens, with mobile internet promising to double that number; data and processes moving to the cloud; an internet of things, with an IP address assigned to your refrigerator; business and government digitizing their core processes, and here in Estonia, even online national elections.

The physical and the cyber worlds are quickly converging and boundaries between the "cyber" and the "real" world have begun to disappear. This in turn implies a convergence between cybersecurity and overall global security. We already have witnessed one real case of cyber-kinetic convergence in the Georgia-Russia War.

To understand the future direction of cyber conflicts, we must cast a wider glance. At the hundreds of conferences like these that have been held in the past decade, the focus has been much on the technology and far too little on the broader issues and trends, as if nothing similar has ever taken place before. Yet it has. Industrialization in the 19th Century started a process that led on the one hand to the West outstripping the Rest in wealth, a divide challenged only in the past decade. Yet it also created the tools for the industrialization of death in World Wars I and II. Technology matters strategically, politically and morally so we need to keep in mind the bigger picture and what is at stake when we discuss different societies' and countries assumptions about the nature of the cyber world. These assumptions determine how the internet will be used.

Like it or not, we have now entered a new period of struggle between competing systems of government and economic organization. This time, there is no Iron Curtain, no statement of hostilities, no declared conflict of ideologies. What is at stake in this struggle is the liberal-democratic model of an open society and market economies that are transparent and rule bound. This time, the struggle will play itself out in cyberspace. Perhaps, it will remain be a global cold peace, but a cold one nevertheless.

This is a struggle we find ourselves surprised to be engaged in. Twenty years ago, we argued whether history was eventually to end with near universal assent to the principles of liberal democracy and competitive market capitalism. The events of the 1990s seemed to bear this diagnosis out. The formerly Communist countries of Central and Eastern Europe, Latin American and Asian countries joined the family of liberal democracies. Where democracy had not yet prevailed, the increasing commercial and informational links of a flat world convinced us it was only a matter of time before it did so.

Our optimism has proven rather naïve, for we did not count on the adaptive cleverness of the competition. The mechanisms of preserving the power of the corrupt and despotic have proven themselves or their elites as a functioning and viable alternative to democracy. This alternative path – authoritarian, often mercantile capitalism – has become for a number of countries the preferred route. We believe still in our implicit neo-hegelianism, that these are but temporary setbacks in the ineluctuable march of history toward democracy. That a middle class will rise up and protest. And we see in the overthrow of despotisms a vindication of our hopes, yet word is still out whether over-throwing an autocrat necessarily results in his replacement by a democratic government. Were these countries simply poor and ruled by rent-seeking authoritarians, this would not perhaps bother us so much. But authoritarian capitalism well endowed with natural resources, i.e. petro-states with corrupt yet efficient secret police, combined with muzzled journalism, or with plentiful cheap labor, has flourished under the conditions of free trade and other countries' open markets.

Illiberal, non-democracies gain too from cyber

This otherwise old model of political control and collusion between government, business and crime, whether you call it reformed communism, crony capitalism, sovereign democracy, the Beijing consensus or just plain despotism, has gained a new lease on life in or through cyberspace. We in the liberal democratic West, in countries with low scores on the Transparency International Corruption Index, have built a solid firewall between the private and public sectors. Even the term Public-Private Partnership attests to the relative separation of the two. No such separation in mercantilistic or authoritarian kleptocratic regimes exists. One serves the other.

The net has been a double-edged sword for the democratic activist or investigative journalist in a non-democratic society. Egyptian and Tunisian citizens left no doubt in their words, their deeds, their protest marches and prayers, that they yearn for freedom and democracy. The internet is a tool for Russians, Chinese, Iranians to learn about the outside world (and via that their own world), to document government corruption and misbehaviour, post their anger and disappointment, discover the like-minded and debate over disagreements.

Yet as we have seen in the past years, the internet can also strengthen the hand of savvy authoritarians and mobsters, allowing them to track their citizens, squash protests, censor dissent, and bully their people. At the same time, these countries and their criminal networks can serve as a web-enabled base of operations for globalized networks of smuggling, money laundering and intellectual property theft.

If these countries oppressed only their own citizens, we might satisfy ourselves with an attitude of benign neglect. Yet these countries' elites have realized they can put their fingers on the economic scales to tip them in their own favour. Intellectual property, R&D investments both public and private, make modern Western economies run. A Western company that invests hundreds of millions or billions in new products can see this all evaporate if the research is stolen. (Recent US Congressional testimony by former FBI Assistant Director Shaun Henry gives some examples.) Someone, somewhere else, can obtain for free what your country's best and brightest have developed, often from years of research. The innovator loses his investment, your country loses the tax revenue, and someone else reaps the profits. This is piracy. Pure and simple. It is as dangerous and as threatening as earlier, more primitive forms of piracy off the Barbary Coast at the beginning of the 19th century, or today off the coast of Somalia.

And it will only get worse.

Cyberspace: a power vacuum

It took the West 350 years to get from Thomas Hobbes' description of anarchy in 17th century Europe - a "war of all against all", in which life is nasty, brutish and short – to a consensual model that assigns monopoly to sovereign states on the use of force within borders, and to develop institutions and norms to mitigate international anarchy. At our current rate of progress, perhaps best described by Moore's Law, we don't have that time.

At its worst, cyberspace now resembles a Hobbesian state of nature. Our national and international institutions have failed to prevent a continuous low-level insurgency of crime, both organized and unorganized, terrorism, state-sponsored attacks and cross-border vigilantism, state-organized as well as ad hoc (viz. Anonymous and LulzSec).

There are many reasons for this effective power vacuum in cyber space, most of which you have discussed this week. But I would like to add one more possible and more fundamental explanation into the mix: The open structure of the internet forces countries with irreconcilable domestic political arrangements into almost inevitable conflict. Borders no longer contain bad behaviour, states no longer are held responsible for illegal actions emanating from within their territory.

Look at it from the perspective of an authoritarian government that needs to maintain its power structure and placate its stakeholders and private sector partners while preventing a democratic revolution. Up to the internet age, the Westphalian system, cuius regio, eius religio and the principle of the inviolability of borders protected the regime. A ruler could do as he wished, so long as he stayed in his own borders.

In cyberspace, these countries are faced with the import of potentially disruptive liberal aspects of open societies. The means of expression, transparency and accountability empowered by a Google search, a YouTube video, or a tweet are a direct threat to a non-inclusive economic and restrictive political system; the World Wide Web turns them into domestic threats to the regime. So, these governments must rely on filtering and blocking, using sophisticated monitoring and filtering software while co-opting internet companies operating in their country. When these methods fail, they cut off the internet wholesale, as the Mubarak regime did in Egypt.

Unfortunately for us, the openness of the internet also means our own citizens are no longer isolated from the violence, corruption and illiberalism of others' domestic spheres. These regimes, and actors under their protection, use - with near impunity – the same tools against Estonians or Americans that they employ against their own citizens and companies. During the Cold War, Communist leaders may have been frustrated by the freedom within Western countries, but there was a limit to what they could do about it. Today, they can deface your website, DDoS your server, hack your email, steal your data, identity and financial information, spy on your friends, plant malware in your company or government, exploit your industrial control systems, and so on. Our strength – our openness – is at once also our greatest liability. This is the crux of the challenge we face. This is especially true in a small country like mine that Freedom House ranks number one in the world in internet freedom.

We must choose between two paths – either we can change the nature of the internet by placing a Westphalian regulatory structure on internet governance, or we can change the world.

The SCO and CIS countries prefer the former. Authoritarian kleptocracies may benefit from anarchy in cyber space but, even more, they fear the West is attempting to orchestrate an Arab Spring or an Orange Revolution. This helps explain why illiberal states want to develop new regulations for the internet, to put another brick in the wall (or is it another wall in the BRICs?), expanding their Westphalian space to cyber. This would be sovereignty on their terms, disabling the freedom and sovereignty of our citizens and businesses.

This December, in Dubai, the International Telecoms Union will hold its first world conference since 1988. 24 years is a millennium in cyberspace. The outcome of this conference, and related processes, will help determine the topography of the web for the next two decades. While this conference may fall into the domain of ministries of commerce and communications, make no mistake, there will be major cyber security ramifications. More ominously we will face calls to limit free expression as we know it on the web today.

The CIS and SCO will again present proposals that would undermine the current multi-stakeholder model of the internet, replacing it with a scheme that would allow them to expand their control of their own populations and economies extending it to undermine the freedom and openness we value today. They will claim that sovereignty in cyberspace is necessary to rein in cybercrime and cyber-terrorism.

Reality belies that claim. International legislation to combat these problems is long in place – in democratic countries. Thus to be a cyber-criminal or hacktivist in Estonia or United States is a dangerous proposition. Last November, a joint operation between the FBI and the Estonian Security Police culminated in the apprehension of the botnet and spyware group Rove Digital, the largest arrests of cyber-criminals to date anywhere in the world. Similarly, law enforcement has had no problem putting illegal file-sharing site Megauploads out of business or picking up the lead hackers of Anonymous. For some reason, our requests for legal assistance to go after similar criminals in China, Russia or Iran mostly go unanswered. The world doesn't need more sovereignty, it needs countries to actually exercise the sovereign control they already have.

The world is not clearly divided into two camps on this matter. Between the US, the EU and like-minded nations at one end of the spectrum, and authoritarian countries at the other extreme, a large number of countries sit on the fence on the issue of the future architecture of the internet. They have legitimate concerns about internet governance, so we must focus our attention on their needs while reassuring them about our actions and intentions.

I would conclude with five observations on how to proceed:

First, we must fully embrace the information society

• The 20th century paper-based, brick and mortar bureaucratic administrative state is a legacy technology. Today, in Estonia, I can start a business, scrutinize my medical records, sign contracts and even vote from my desktop. And our innovation in public-sector IT is only the tip of the iceberg to massive changes that will disrupt government as much as the information technology already has in the private sector.

- New uses of technology will create new security risks. These risks will require us to use strong security and an architecture like the Estonian x-road that enable authentication, digital signatures and interactions more secure than their paper equivalent. Countries that fail to give their citizens a digital ID of equivalent states to a paper ID are luddites, pure and simple.

- We need to harness the potential for disruptive change and extend the digital society across borders. Last year, over 1000 Finnish entrepreneurs started businesses online in Estonia using their Finnish electronic ID card. This is only a tiny example of how we could integrate business and societies across borders. The hurdles are today bureaucratic and political, not technical.

Second, be pragmatic and learn from models that work

- We have many lessons to learn from the successful war on terror. In the ten years since 9/11, we have achieved a level of international law-enforcement and intelligence cooperation and operational proficiency that would have been inconceivable in the 1990s. Why can't we achieve the same in cyberspace?

- Both domestically and internationally, we need to use the organizations and structures we already have, adapting them to new challenges. A good example is the Estonian Cyber Defence League. We took our existing Defence League, a voluntary structure analogous to a national or home guard, and brought together private and public sector cybersecurity experts the state could never afford to hire, but who are willing to volunteer their time and effort for free out of patriotism.

Third, embrace Radical transparency

Liberal-democratic, free societies can best meet a security threat when they adopt an ethic of openness and transparency.

• One of the strategic choices Estonia made in 2007 was to be very open about cyber attacks. This brave public acknowledgment of our weaknesses made us stronger, and made the world more aware of cyber threats; made the world safer.

• The key to cyber defence, even against sophisticated state actors, is civilian cyber-security. Cyber attacks are such an attractive option for our adversaries because they neutralize the West's conventional military superiority, targeting our personal data, banks, utilities, sources of information and confidence in our government. For this reason, our center of gravity must lie in raising the security savvy of our private sector and individual users.

• This in turn requires openness and sharing. Detailed intelligence about APT-s and SCADA vulnerabilities isn't useful if it's marked TOP SECRET and potential victims don't find out about the threat until it is too late. Openness and transparency is in the DNA of our societies, so let's leverage that advantage.

Paradoxically, openness and transparency is a tactic that can even work for the adversaries of the World Wide Open Society. The Iranian CERT released the code for the Flame virus, and within some weeks, several European teams had analyzed the malware, reverse engineered it and designed patches, so that in effect the Iranians, using openness, piggybacked on the cooperative community that has developed in our free societies to increase their own security.

Fourth, let's get our act together on international cooperation

We've been talking about international cooperation in the cyber domain since 2007, but we have a long way to go. In NATO, we will only reach the bare minimum acceptable level, defending NATO's own networks and N-CIRC FOC, in 2014. But NATO lacks a more ambitious vision for a post-2014 period. And in the EU, we still do not have a comprehensive approach to cyber-security.

Sadly, these are also not auspicious times to speak of the transatlantic link.

• Barack Obama is the US' first Pacific President, but the US military's shift toward Asia is a long term if not permanent change that will continue under any administration. Within Europe, we are having difficulty meeting the basic commitment to meet NATO's requirement of spending 2% of GDP on defence, which only a few Allies do.

• Austerity measures have also made it more difficult to speak of major European investments into cyber-security.

This is misguided. Investments in conventional defense, where there have been few advances in the last decade perhaps can bear with austerity. Failure to invest in a realm changing by leaps and bounds is simply foolish and for governments and innovative companies, irresponsible.

Mostly, I worry about international cooperation actually becoming less open and flexible. The international network of CERT-s that grew out of the academic world in the 1990s was flexible, decentralized and open. In recent years, as countries have made cyber-security a matter of national security, they have focused capability development in military and intelligence organizations, complicating international cooperation instead of encouraging it.

If we do not change course, we will exacerbate a fundamental mismatch between what we must defend internationally – economies and lives that cross borders, especially in the EU – and the mostly national means we are using to achieve this goal.

Finally, this audience must develop a clear community ethic

You are no longer practitioners of an obscure, technical area. Prime ministers, CEOs and your voters and consumers are looking to you for answers. You have responsibility for giving good advice and making prudent decisions and if you screw up, we will all suffer. So it's time to think about hard questions:

- What is your standard of evidence for a good argument, good advice?

- How do you insure you are listening to dissenting voices?

- How do you ensure accountability?

- What is the role of industry within the academic and policy world?

To sum up

I believe that liberal democracy, open markets and accountable institutions can prevail today as surely as they did during the Cold War. But we do not live in a deterministic world. Success will demand good people to do smart things, and the price of hubris and misjudgment could well be failure.

Ultimately, what is it that we're talking about when we say international cooperation, openness, and so on? Our countries, our companies, our analysts – they form a network. In addition to the physical network and the software running on it, there is a network of organizations and people.

If a network consists of many connections between nodes, and information travels quickly between the nodes, the network will be flexible, resilient and quick to react. The internet is such a network, as is the human brain.

International cooperation, information sharing, openness and transparency, the comprehensive approach, public-private cooperation and so on are not just polite words. They are part of building a collective brain that leverages the fundamental, inherent advantages of free, open societies. At its best, this collective brain could be far more intelligent, far nimbler, than any adversary, any threat. For this collective brain to work, however, we have to allow the synapses to fire, and we have to allow neural pathways to develop across organizational and international boundaries.

If, on the other hand, we bottle up information, erect barriers, and treat cooperation as a formality, we lobotomize ourselves. Put another way, we fail to learn from the open and decentralized architectural principles of the internet. And we will lose.