

by Nicholas Hirst

Estonia's president singles out trust as the key ingredient for building a robust internet for the future, although trust itself seems to have been lacking between EU member states over a proposal on cyber security.

Toomas Hendrik Ilves, the president of Estonia, recently sounded a warning on cyber-security. "We need to work toward and reach agreements on the norms of behaviour regarding the cyber world and develop adequate defences against those that do not accept the norms of openness and freedom," he said at a conference in Tallinn on 4 June, organised by a NATO research centre. Estonia is a country renowned for its take-up of digital technology.

The "dystopian alternative" was that European societies and industries would go the way of the defence industries: fearful of potentially disastrous security breaches they would retreat behind national defences. Indeed, cyber-attacks and defence are increasingly "part of the larger world of competition between states, of interstate and economic relations", he continued.

However, Ilves (pictured), a former MEP, did sound a note of optimism. Liberal democracies can, he argued, build legal frameworks that would increasingly prove "the basis for economic policy" provided they "restore and re-establish what has been lost: trust among allies".

Yet among European Union member states – leaving to one side the case of the United States following the revelations of Edward Snowden – that trust will prove elusive in the short term. That much was in evidence on Friday (6 June), as EU telecoms ministers debated the European Commission's proposal to bolster EU cyber-security.

Under the draft rules, member states would be required to set up national authorities dedicated to ensuring network and information security and creating emergency response teams for breaches. But it is provisions that would oblige member states' agencies to exchange information among themselves that are proving the main sticking point in negotiations.

Germany, the United Kingdom, France, Spain, Sweden, Finland and Ireland lined up to reject such exchanges. The EU "first needs to create the conditions for trust" before mandating it, observed Alexis Duterre, France's deputy permanent representative, whose comments were echoed by several ministers.

This was in stark contrast to the position advanced by central and eastern European member states. "Cyber-security is indivisible" and co-operation "indispensable for EU-wide security", said Rafał Trzaskowski, Poland's minister for administration and digitalisation, in echoing his Czech counterpart.

Estonia's Clyde Kull, the country's deputy permanent representative, agreed. The major cyber-attack suffered by Estonia in 2007 had taught it the importance not just of co-operation, but of operational co-operation. The EU was "lagging behind," he warned.

Will EU telecoms ministers heed the warnings of the bloc's most connected member? Elsewhere, Estonia's warnings have not fallen on deaf ears. Ilves warned in a speech in Washington in 2012: "To impoverish a country you simply erase their bank records." Just on Tuesday (10 June), the Bank of England announced that it would start stress-testing UK banks' cyber-attack defences.

Original article on the European Voice [webpage](#) .