

By Chris Glew

President Ilves today addressed the All-Party Parliamentary Group on Homeland Security in the UK House of Common, upon the invitation of its treasurer, James Morris MP.

The key theme of the President's remarks was identity and, more specifically, who should be responsible for securing and guaranteeing it in society. He outlined the concepts of DDOS attacks and how they had been used to target Estonia in 2007. Asked by former UK Security Minister Baroness Neville-Jones on how vulnerable he considers Western nations to cyber-crime, he commented that the issue is more problematic for the "English speaking peoples" who are often more nervous about the role of identity and identity management. He suggested that whereas only governments previously had the monopoly on military force, it should now take on the role of guaranteeing the identity of its citizens and that a cultural change was necessary. On the subject of data ownership he outlined that in Estonia the citizen owns the individual data about him or her and that any abuse of that data would be regarded as an abuse against the person itself.

Neville-Jones however put forward the argument that whilst the threats are very real, the power of the state should be limited and it is the responsibility of the citizen to take steps to protect their identity. Ilves countered with the analogy of market failure – when a bank encounters financial trouble, the government steps in to resolve the issue. Similarly, when banks or other enterprises suffer losses due to cyber-crime or digital fraud, this should also be regarded as a market failure and the government should step in to ensure the integrity of the system.

Former British Foreign Secretary Sir Malcolm Rifkind put to President Ilves that some have been quoted as saying as much as 80% of the cyber-crime which troubles society could be defeated – Ilves replied that a higher proportion could actually be stopped with the right techniques and strategies. He made reference to the US Department of Defense Security Technical Implementation Guide – whereas the US has managed only to fulfill several criteria, Estonia has met them all and has done for some time. On the subject of state sponsored cybercrime, he noted the problem of third party aggression being carried out on behalf of other states. The problem lies in identifying who is behind the attacks.

He warned about about mobile apps and the effect on personal data. Whereas people are guarded about the state having access to their information, they willingly hand over statistics based on their own movements or personal health to mobile apps which then seek to monetize them in less than obvious ways. Citizens are often, understandably worried about "Big Brother" but perhaps they should also concern themselves with "Big Data" he said – personal information that is collected in surreptitious ways and used for targeted advertising and profile building. "There's no such thing as a free app", he joked.

Yesterday Ilves spoke at the influential Google Zeitgeist on the subject of Open Data and transparency. He returns to Estonia this evening.

Original article on the Estonian World [webpage](#) .