The Estonian President and Baroness Neville-Jones in Conversation on Cyber Security

https://www.e-ir.info/2013/06/02/the-estonian-president-and-baroness-neville-jones-in-conversation-on-cyber-security/

RACHAEL SQUIRE, JUN 2 2013

Last week, the President of Estonia, Toomas Hendrik Ilves visited Parliament to discuss the threat of cyber security in the 21st century. Co hosted by the Henry Jackson Society and the APPG for Homeland Security, the President was joined by Baroness Pauline Neville-Jones in what turned out to be a fascinating discussion about personal freedoms, liberty and state power.

Both speakers came with a wealth of experience on the issue – Ilves in particular having presided over the first politically motivated cyber attacks on a country in 2007 when Estonia was hit by a barrage of Distributed Denial of Service (DDoS) Attacks. Motivated by the removal of the Bonze Soldier Soviet war memorial in central Tallinn, the websites of Government ministries, political parties, newspapers, banks and other companies were disabled as they were overwhelmed by tens of thousands of visits from all over the world. The attacks were a clear sign that one of the most wired countries in the world was also extremely vulnerable.

Estonia has thus had more reason than some to take cyber security seriously – not only because of the attacks, but because of their extensive and world leading cyber infrastructures. As it stands, the country is a beacon of e-governance and a world leader in cyber security. It has invested heavily in digitising the basic possesses of society from tax returns, to prescriptions, to voting at elections. In 2012, over one hundred million digital legal signatures were signed and as citizens legally own their data, they can readily access things like their health and dental records online. The Baroness stated that we are in an age where 'data has now become your being', sentiment shared by Professor Choucri who stresses the impact of cyberspace on the human condition, arguing that it has "created a new reality for almost everyone and everywhere", Estonia proving a case in point.

Both speakers agreed that cyber security is an issue of paramount importance for every country, not just those who are as wired as Estonia; their perspectives differed however on who should bear responsibility for this securitisation. On the one hand, Baroness Neville Jones suggests that in the post-cold war era, the individual must bear a greater burden of responsibility. Whilst the Cold War was defined by elevated state power and a passive public in need of protection, we are now living in a time where information technologies have handed power back into the hands of civil society and as such, we all have responsibilities to ensure that the state's security obligations are met. In other words, security is the responsibility of everyone, not just the Government. Speaking at RUSI she stated: "Too many people and organisations still regard responsibility for security generally – and for cyber security in particular – as somebody else's bag; and probably the government's. I don't think that's an attitude that can continue. Altering attitudes to the importance of security and personal responsibility for it and in it is one of the tasks that lies ahead of us."

On the other hand President Ilves stressed that the state must fulfil its primary function of securing its citizens in the cyber world as well as the physical world, and more importantly, that the public should trust their Government to do so.

The success of Estonia's cyber governance infrastructure has been facilitated by the Government's commitment to authenticating the identities of its citizens. The Estonian Government have become the guarantor of secure online

transactions using a two-factor identification system in which ID is protected by both a chip and password. This 'public key infrastructure' guarantees the secure transfer of information – a system that remained intact even during the attacks of 2007. The reason for this system is so people can know exactly who is communicating with them. In a Hobbesian world with 'bad neighbours all around', the President stressed the importance of assuring individual identity in tackling cyber security and as the private sector cannot fulfil this security function, the Government must step in to do so. The Government's primary function is after all to provide security to its citizens, yet as Mr Ilves highlighted, people in the Western world remain extremely sensitive to any Government intervention aiming to secure the personal information and identities of their citizens.

Whilst this aversion to big brother governance may have had its place when only national Governments had the ability to monitor their citizens, we are according to Ilves living in a drastically different landscape. Today, a single hacker can access the most personal details of your digital and non-digital life and on a larger scale, hackers, perhaps working with larger organisations use stolen information to launch attacks on critical infrastructure and to steal valuable intellectual property. One publicly traded company in America for example lost $1 billion of intellectual property in a single intrusion over one weekend. In another example, it has recently emerged that the designs for some of the US's most important and sensitive weapons systems have been compromised by Chinese hackers. It is perhaps unsurprising therefore that Obama has announced that cyber security will feature strongly in his visit to China. National Security Staff spokeswoman Laura Lucas also confirmed that there has been a trend over the last year of malicious actors increasing their focus against critical infrastructure. Ilves' point, exemplified in these examples, is that the threat lies with big data, not Big Brother Government.

For the Estonian President, the aim of cyber security is to enable a globalised economy based on the free movement of goods, people, services, capital and ideas. The networked cyber infrastructure, operating more like an ecosystem than individual frontiers, must therefore be protected as a whole and this begins with the securitisation of individual identities. This, is something that Ilves' believes should fall under the remit of the Government. However, as was demonstrated throughout the discussion, some Western countries remain resistant to Government interference with personal data. We saw this sensitivity in this country when former Prime Minister Gordon Brown suggested the introduction of Identity cards. To adopt Ilves's standing on this issue, cyber security is thus an issue dependent on certain cultural norms as well as practical defence systems.

Looking to the future of cyber security in Europe and indeed the wider world, both the Baroness and Estonian President highlighted some interesting points. Firstly, with regards to Europe, Western states should be following the example of Estonia in terms of how seriously cyber security and cyber infrastructure is taken. Only when European countries have caught up with 'E-stonia' can government data move as freely across borders as emails, adding an entirely new dimension to the phrase digital diplomacy. Whether other European countries would want such integration is another matter entirely.

Both speakers also highlighted a need for innovation and forward thinking in NATO's response to cyber attacks. Of course, this is made all the more difficult by the often ambiguous nature of attacks but both the Baroness and President stressed the need to stop conceptualising cyberthreats in military, or classical warfare terms. At one extreme, cyber attacks on critical infrastructure can render the military paradigm irrelevant, at another, such cyber attacks will no doubt be combined with kinetic attacks in the future, as we saw when Russia invaded Georgia in 2008. NATO thus needs a clear, carefully articulated plan of retaliation to be implemented if a well-orchestrated, state led attack does occur. Cambridge University Press have recently published a NATO manual for cyber warfare, however, as the article states, this is an advisory document, meaning that at present, the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to an attacked country.

Had there been more time, the discussion and questions from the audience would have continued well into the afternoon. Both the President and Baroness proved to be extremely insightful speakers, challenging the audience to re-examine many of our assumptions about security, state power, and civil liberty. In a landscape where the relations between the public and private spheres, between privacy and identity are shifting, it is inevitable that the realms of cyber security and overall security will converge. This convergence, if Ilves' insights are correct, may well be a

turbulent one as Government's seek not only to ward off attackers, but to overcome deep seated domestic cultural barriers which lend themselves to fierce protection of privacy and a strong aversion to anything resembling a big brother state.

—

Rachael Squire *is working towards an MSc in Geopolitics and Security at Royal Holloway as part of her ESRC funded PhD studentship on the geopolitics of rumour and conspiracy. Rachael also works part time for a Member of Parliament. Read more of GPS: Geopolitics and Security – Critical Perspectives From Royal Holloway.*

About the author:

Rachael Squire is a first year PhD student in Geopolitics and Security at Royal Holloway University of London. Her research focuses on underwater geopolitics and mobilities, ocean space, materiality, and sound. Rachael co-edits the blog rhulgeopolitics.wordpress.com