LINK centre

Learning Information Networking Knowledge

Faculty of Humanities
University of the Witwatersrand

LINK Centre Annual Lecture 2019

Ewan Sutherland discusses Global Cybersecurity Developments

Respondent: Kiru Pillay, Chief Director: Cybersecurity Operations, Department of Communications

Source: Wikimedia Commons, https://upload.wikimedia.org/wikipedia/commons/4/46/Cybersecurity.png

Accelerator North, Tshimologong Digital Innovation Precinct, 41 Juta Street Braamfontein

Tuesday 20 August 2019 17h00 – 18h30

RSVP to Nokhanyo Yolwa at nokhanyo.yolwa@gmail.com

There are sophisticated markets for cybersecurity products and services, for example banking, financial services and insurance, and many other sectors in business and government, which are tracked by periodic analytical reports. Yet these markets have significant flaws that have led to legislative and regulatory interventions, in particular addressing negative externalities, where the costs of failures fall on firms, organisations and individuals with little or no incentive to pay in advance for more robust systems.

The WannaCry malware attacks in May 2017 pointed to failings of governance and management in the United Kingdom National Health Service (NHS), arising from poor assessments of cybersecurity and insufficient planning. A parliamentary inquiry helped identify remedial actions, whereas the intelligence services took seven months to attribute the attack to North Korea – too late for an effective response. The European Union has applied its conventional political approach to cybersecurity, developing incremental legislation and policies, building on successes and sharing lessons (e.g., the attack on Estonia). Member states have agreed to create a series of governance networks linking cybersecurity functions in government, in the judiciary, the police and in national cybersecurity centres. This helps slower moving member states and has sought to balance human rights with increased security. Globally initiatives are underway at various international fora, and at the UN, to establish global frameworks for cybersecurity governance including the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG), however many committees and institutions are making slow progress. Brexit or the departure of the United Kingdom from the EU has been delayed but will, if and when completed, remove it from EU legislative and policy procedures, including a range of networks that have allowed agencies and departments to support the development and implementation of cybersecurity measures. These include national CERTs, police forces, judges and government departments. This does not leave the UK isolated, as it remains in Five Eyes (intelligence network), Council of Europe (Budapest Convention and GLACO), NATO and the OECD. However, it does increase the burden on UK institutions and together with other disruptions in government it presents serious challenges in deciding about 5G, IoT and other developments, with much greater responsibility falling on the UK government.

5G had been just another strongly hyped technology platform, generating limited interest from consumers, though claimed to be vital for the Internet of Things (IoT) and machine-to- machine (M2M) communications. Then President Trump denounced Huawei as an agency of the Chinese Communist Party (CCP) and a cybersecurity threat to Western nations, banning use of its equipment in the United States. The EU response was cautious, with member states quickly conducting national risk assessments, with an EU-wide risk assessment and unified mitigation measures expected by the end of 2019. Very few countries are expected to follow the US in banning Chinese equipment from 5G networks, many suspecting it is a trade rather than a cybersecurity issue.

Considerable attention has been given to the opportunities from the Internet of Things (IoT), with work on deployment and spectrum. The secure by design (SbD) part of the GDPR is expected to reduce some of the risks, but much work is expected to identify problems and to feed into iterative legislation. Nonetheless, there are considerable risks to privacy from weak cybersecurity of increasingly ubiquitous IoT devices. Initiatives to boost ICT skills more generally now have explicit strands for cybersecurity at all levels, from educating the general public about scams through to postgraduate courses in digital forensics.

Cybersecurity is a difficult area for governance, given technical advances, unknown capabilities of some actors, especially APTs, and the need to coordinate so many individuals, families, firms and organisations. What are the lessons for South Africa?

Ewan Sutherland is an independent telecommunications policy analyst who has undertaken assignments in Asia, Southern Africa and Europe - for governments, World Bank infoDev, the International Telecommunication Union (ITU), and the Organisation for Economic Co-operation and Development (OECD). He publishes on a wide range of telecommunications topics: http://ssrn.com/author=927092