NZ-UK joint statement on cyber security

beehive.govt.nz/release/nz-uk-joint-statement-cyber-security

16 January 2013
Murray McCully

Foreign Affairs

Overview

1. Cyberspace is one of the greatest national, global and strategic challenges of our time. Cyber intrusions are an increasing challenge for the security of systems and networks of national importance. New Zealand and the United Kingdom are already working closely together to confront the growing threats we face to our cyber security, and it is vital to our wider, shared economic, security and defence interests that we do so. We are clear that our success in this sphere will be fundamental to our joint realisation of the transformational opportunities that Cyberspace offers.

2. New Zealand and the United Kingdom share a common position on the core principles of liberty, transparency, freedom of expression and the rule of law in cyberspace. Through our respective National Cyber Security strategies we have each set out our responsibility to protect our core Government systems, systems supporting our critical national infrastructure, and the need to work with industry and business as key partners in establishing a safe digital environment for all.

Policy Coordination

3. New Zealand and the United Kingdom have a long history of cooperation on policy, defence and security based on our shared values and principles. Policy in cyberspace is complex and requires coherence across government and collaboration with close allies and the wider community. Responding to the most challenging threats will require difficult policy choices.

4. We will work jointly, and with our allies, to further develop a vision for the future security of cyberspace and will work together to advance this through positive international engagement.

International Engagement

5. We do not underestimate the challenges ahead in working with the international community to achieve consensus on how to protect the cyberspace and, within that, the internet which has been an unprecedented engine for growth, social progress and innovation across the globe and in all areas of human endeavour.

6. New Zealand and the United Kingdom will work closely together in relevant international fora to advance common understanding on the importance of an open, dynamic Internet underpinned by the body of applicable existing international law.

7. We recognise the gap between supply and demand for cyber security capacity building internationally. The United Kingdom, through the establishment of a new Global Cyber Security Capacity Building Centre (GCSCBC) is looking at how to make better use of the skills and resources internationally to address this issue.

8. The United Kingdom and New Zealand will work closely together to ensure these and other efforts can attain full global reach, including how to best support the work of the ASEAN Regional Forum partners and also the Pacific Island Forum's regional security committee.

Economic Benefit and Business/Government Partnerships

9. Security and resilience of our networks and promoting a safe digital environment requires our governments to build and maintain a close working relationship with the private sector that manufactures, owns or operates the majority of infrastructure on which the global internet relies. We will look at opportunities for increased New Zealand – United Kingdom exchange on our respective business outreach programmes and through that improve links between our key industry partners.

10. We also need to work closely with the business community generally, to build awareness and to improve companies' ability to take responsibility for protecting their intellectual property. Creating a cyber-aware investment environment is essential if we are to create the conditions for business success, and help our companies respond to the challenge of globalisation.

11. We will collaborate on cyber-related research and development activities, both within government and with the private sector in both countries.

12. We will explore the potential for synergies arising from our respective cyber investment programmes. Where appropriate, we will work jointly to deploy new capabilities and will share our thinking on the development of new approaches to government partnerships with the private sector.

Mutual Defence

13. We will continue to share situational awareness information and intelligence and security data from a wide range of sources to maximise the ability of both nations to detect and respond to foreign cyber intrusions on networks of national importance.

14. We will work closely together, and with our key allies to coordinate responses to incidents affecting our government and private sector networks.