# Press release: Joint UK-Australia Statement on Cyber Co-operation

The UK and Australia enjoy a historic relationship and modern partnership. It is a unique and enduring bond built on friendship and shared values; one underpinned by strong security, prosperity and people-to-people links; one more relevant than ever as we work together advancing common interests and tackling global issues, including in cyberspace. We recognise that the pace and development of new technologies and applications, in conjunction with greater access, is delivering significant opportunities for both economic and social development. While bringing great advantages, the reliance on increasingly interconnected networks also exposes states to new vulnerabilities. Irresponsible or illegal exploitation of those vulnerabilities can have both profound impact on the victim and, in the most egregious cases, risk international stability.

We confirm our joint commitment to promoting an international stability framework for cyberspace based on the application of existing international law, agreed voluntary norms of responsible state behaviour and confidence building measures, supported by co-ordinated capacity building programmes.

Australia and the UK will co-operate to deter, mitigate and attribute malicious cyber attacks by criminals, state actors and their proxies, including those that seek to interfere in the internal democratic processes of states. We will work with industry to implement resilient cyber security solutions for their products and services. We will also share lessons learned as we develop measures to provide defences across our governments, and make it easier for individuals and organisations to stay safe online.

We reaffirm our commitment to a free, open, peaceful and secure cyberspace. The foundation for responsible state behaviour in cyberspace is our mutual commitment to existing international law, including the respect for human rights and fundamental freedoms, and the application of international humanitarian law to cyber operations in armed conflict. We reaffirm that the UN Charter applies in its entirety to state actions in cyberspace, including the prohibition of the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in self-defence in response to an armed attack (Article 51). The law of state responsibility applies to cyber operations in peacetime, including the availability of the doctrine of countermeasures in response to internationally wrongful acts.

We recognise that an increasing number of states are developing operational cyber capabilities. We assert states’ legitimate right to develop these capabilities, and emphasise their obligation to ensure their use is governed in accordance with international law. Acknowledgement of these capabilities does not encourage aggression, or contradict our common commitment to maintaining a peaceful ICT environment. Rather, acknowledging the existence of these capabilities fosters the understanding that, just like in the

physical domains, states’ activities in cyberspace do not occur in a vacuum – states have rights – but they also have obligations.

We will promote operationalisation of norms of responsible state behaviour recommended in the 2015 report of the UN Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security. We will focus on positive practical measures that states can take to put these voluntary norms into practice. We will also implement confidence building measures that can build trust between responsible states. In doing so we recognise that transparency is the first step to establishing mutual trust and provides a foundation for measures available to all states, whatever their stage of development. We are committed to working through the OSCE and ASEAN Regional Forum as a way of contributing to peace and understanding in cyberspace.

We confirm our mutual commitment to cyber security capacity building that directly contributes to international stability: recognising the importance to all our security of states developing responsible legal and governance frameworks, overcoming the barriers to implementing agreed norms, building resilience to cyber threats, and strengthening law enforcement responses in line with the Budapest Convention on Cybercrime. As the next 1 billion people access the economic and social benefits of cyberspace, it is in all of our interests to ensure that cybersecurity is understood as a key part of the development agenda.

## Further information