WRITTEN MINISTERIAL STATEMENT

CABINET OFFICE

25 November 2011

Minister for the Cabinet Office and Paymaster General: The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World

---

Francis Maude

I have today published the new Cyber Security Strategy for the United Kingdom. I have placed a copy in the Library.

The growth of the internet has transformed our everyday lives.

But with greater openness, interconnection and dependency comes greater vulnerability. The threat to our national security from cyber attacks is real and growing. Organised criminals, terrorists, hostile states, and 'hacktivists' are all seeking to exploit cyber space to their own ends.

This Government has moved swiftly to tackle the growing danger posed by cyber attacks. Our National Security Strategy published last year classed cyber security as one of our top priorities alongside international terrorism, international military crises and natural disasters. To support the implementation of our objectives we have committed new funding of £650m over four years for a transformative National Cyber Security Programme (NCSP) to strengthen the UK's cyber capabilities.

The new Cyber Security Strategy we have published today sets out how the UK will tackle cyber threats to promote economic growth and to protect our nation's security and our way of life.

One of our key aims is to make the UK one of the most secure places in the world to do business. Currently, around 6 per cent of the UK's GDP is enabled by the internet and this is set to grow. But with this opportunity comes greater threats. Online crime including intellectual property theft costs the UK economy billions each year. So we must take steps to preserve this growth, by tackling cyber crime and bolstering our defences, to ensure that confidence in the internet as a way of communicating and transacting remains.

The Government cannot tackle this challenge alone. The private sector - which owns, maintains and creates most of the very spaces we are seeking to defend – has a crucial role to play too. This strategy outlines how we will cement a real and meaningful partnership between the Government and private sector in the fight against cyber attacks, to help improve security, build our reputation as a safe place to do business online, and turn threats into opportunities by fostering a strong UK market in cyber security solutions.

Together with the private sector, we are pioneering a new national cyber security 'hub' that will allow the Government and businesses to exchange information on threats and responses. This promises to transform the way we manage cyber attacks and greatly strengthen our security capacity. We will work with the business services sector to raise industry awareness. We will also work with industry to develop private-sector led standards for cyber security that help consumers navigate the market in security products and give firms who are good at security the means to make it a selling point.

The UK is a world leader in cyber security research, development and innovation. GCHQ is the lead in this area and the new strategy aims to capitalise on this through an innovative approach which will explore options with UK industry to harness this expertise and know-how for the benefit of the UK economy.

This strategy also outlines our plans for a new Cyber Crime Unit with the National Crime Agency, to be up and running by 2013. This unit will build on the ground-breaking work of the Metropolitan Police's eCrime Unit by expanding the deployment of 'cyber-specials' giving police forces across the country the necessary skills and experience to handle cyber crimes. We will also ensure that the police use existing powers to ensure that cyber criminals are appropriately sanctioned as well as introducing a new single reporting system to report financially motivated cyber crime through the existing Action Fraud reporting centre.

To defend against significant threats we need to continue the work we are doing to protect and prepare our Critical National Infrastructure. We also need to update our military defence capabilities for a new cyber world; this strategy outlines the creation of a new Joint Cyber Unit hosted by GCHQ which will develop our military capabilities to give the UK a comparative advantage in cyberspace.

We will also strengthen the role of the Centre for Protection of the National Infrastructure to increase its reach to organisations that have not previously been considered as part of the critical infrastructure thereby augmenting our ability to protect critical systems and intellectual property.

Prevention and education are also crucial. Get Safe Online is a very good example of how government, industry and law enforcement can work together to address this issue and improve the website by early 2012. In addition, we will work with ISPs to seek a new voluntary code of conduct to help people identify if their computers have been compromised and what they can do about it.

Cyber risks are transnational in nature. We will work with other countries to tackle them. Through the London Cyber Conference, hosted by the Foreign Secretary earlier this month, the UK is taking a lead in addressing international discussions on how we can establish a more focused international dialogue to develop principles to guide the behaviour of Governments and others in cyberspace. We will continue to foster this level of international dialogue through various fora and through international cooperation on tackling cyber crime.

This strategy sets out the change that is needed; we now need to work together to deliver it. The Government will update the House in a year's time on how we are doing.