Fact Sheet 18: Cyber Security

The UK must address new threats and risks in cyber space

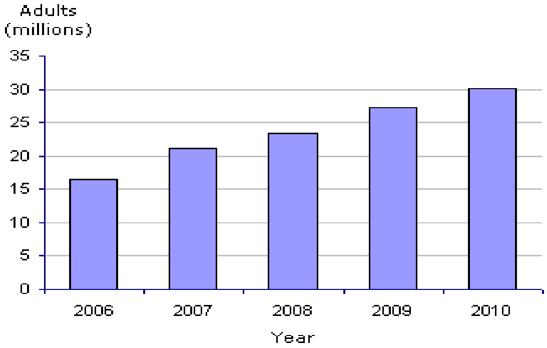
The risks from cyber space (including the internet, wider telecommunications networks and computer systems) have been identified in the National Security Risk Assessment as a Tier One risk. This means that they are judged to be one of the highest priorities for UK national security over the next five years, taking into account both likelihood and impact.

It is vitally important that we protect the UK's interests in cyber space. The internet provides enormous benefits and opportunities for the UK's industries, government and public but as our reliance on it grows, so do the risks and threats we face online

These threats and opportunities are likely to increase significantly over the next five to ten years, as our dependency on cyber space deepens.

Our national security, as well as our economic prosperity, will depend on our ability to protect ourselves in cyber space.

UK internet usage, 2006-10, adults (millions)



In 2010, 30.1 million adults in the UK accessed the internet every day or almost every day (Source: ONS)

Various risks and threats are posed from our increasing dependence on cyber space

Cyber crime is costing the global economy over $1 trillion each year (Source: McAfee)

Using the internet to provide services and for commerce provides undoubted benefits for both the UK Government and industry. This is demonstrated by the continued rise in online spending: in August 2010, UK shoppers spent £4.4 billion online – up 15% over 12 months (source: IMRG).

But the UK is also facing an ongoing, persistent threat from other states, terrorists and criminals operating in cyber space, which needs to be guarded against. For example:

- there are over 20,000 malicious emails on Government networks each month, 1,000 of which are deliberately targeted at them;
- hundreds of hacking forums now exist, and on them thousands of stolen UK credit card details are available for as little as $2 per set;
- cyber techniques have been used by one nation on another to bring diplomatic or economic pressure to bear.

The SDSR puts in place a transformative national cyber security programme, backed by £650 million of new investment

Due to the complex nature of cyber space, improving the UK's cyber security requires a multi-faceted approach involving a close partnership between Government, industry and academia. We will deliver a transformative national cyber security programme, funded with £650 million of new investment over four years, to give the UK a security advantage in cyber security and resilience through:

- overhauling the UK's approach to tackling cyber crime, including through the introduction of a single point of contact where the public and businesses can report cyber crimes;
- addressing deficiencies in the UK's ability to detect and defend itself against cyber attack by improving our ability to deliver cyber security products and services; and enhancing our investment in national intelligence capabilities;
- creating a new organisation, the UK Defence Cyber Operations Group, which will mainstream cyber security throughout the Ministry of Defence and ensure the coherent integration of cyber activities across the spectrum of defence operations;
- bolstering the UK's critical infrastructure and vital government networks and services;
- establishing stronger alliances with international counterparts, including by working on a UK-US Memorandum of Understanding to enable us to share information and plan and conduct operations jointly;
- improving national cyber security skills, education and raising awareness through initiatives such as Get Safe Online and the Cyber Security Challenge;
- sponsoring research, in collaboration with the private sector and others to improve our ability to respond to longer term challenges in cyber security.

21st century defence relies on a secure ICT infrastructure

Getsafeonline.org is a joint government and industry initiative to raise awareness of internet security. Another initiative is the Cyber Security Challenge, a public/private sector and academia run competition to help identify and inspire the next generation of UK cyber security professionals

Together, these measures will be developed and brought together in a Cyber Security Strategy to be published in Spring 2011.