International Policy Review Puts Cyber at the centre of the UK's Security

- This week's Integrated Review will commit to a new, full spectrum approach to the UK's cyber capability – keeping our people safe, staying ahead of our enemies and improving the lives of the British people
- The PM will announce the establishment of a 'cyber corridor' across the North of England, creating and sustaining thousands of jobs
- The National Cyber Force is transforming the UK's ability to conduct targeted offensive cyber operations to impose real-world costs on our adversaries

Our ability to detect, disrupt and deter our adversaries while taking advantage of the revolution in the use of smart and cyber technology will be dramatically enhanced by commitments in the Integrated Review of security, defence, development and foreign policy, to be published this week.

The review will set out the importance of cyber technology to our way of life – whether it's defeating our enemies on the battlefield, making the internet a safer place or developing cutting-edge tech to improve people's lives.

Cyber Security is the foundation of our cyber power and the UK has been at the cutting edge of the use of intelligence to disrupt threats online and defend against attacks. We established the National Cyber Security Centre in 2016 to help critical organisations, businesses and the general public protect themselves.

In recent years our adversaries have invested in their own capabilities and are constantly finding new ways to exploit our weaknesses and gain advantage in cyberspace. To cement our competitive edge and keep ahead of our enemies a full spectrum approach is therefore needed.

The Integrated Review will announce a new cyber strategy to create a cyber ecosystem fit for the future, with more investment in education, partnerships with industry and integration across our defence and intelligence services.

The Prime Minister said:

> Cyber power is revolutionising the way we live our lives and fight our wars, just as air power did 100 years ago. We need to build up our cyber capability so we can grasp the opportunities it presents while ensuring those who seek to use its powers to attack us and our way of life are thwarted at every turn.
>
> Our new, full-spectrum approach to cyber will transform our ability to protect our people, promote our interests around the world and make the lives of British people better every day.

The Prime Minister will announce this week that the home of the new National Cyber Force and the nexus of this strategy will be in the North of England, establishing a ‘cyber corridor’ across the region.

Opening the HQ of the NCF in the North of England will drive growth in the tech, digital and defence sectors outside of London and help create new partnerships between government, the sector and universities in the region, placing it in the international centre of cutting-edge developments to keep our people safe.

Defence currently sustains more than 35,000 jobs in the North West of England alone. Digital and cyber jobs will build on the region’s history of being on the cutting edge of defence technology – 10,000 people are employed in maritime design in Barrow and 12,000 people work in advanced aerospace engineering and manufacturing at Samlesbury Aerospace Enterprise Zone, where the UK is producing the fifth generation F-35 stealth aircraft.

The North of England is already home to a GCHQ office in Manchester, which is and is Europe’s fastest growing major tech cluster, with more than 15% of Manchester’s population employed by the digital, creative and technology sector.

The National Cyber Force was created last year to transform the UK’s capacity to conduct targeted offensive cyber operations against terrorists, hostile states and criminal gangs. It draws together personnel from both defence and the intelligence agencies under one unified command for the first time.

The kinds of operations the NCF is able to carry out include:

- Interfering with a mobile phone to prevent a terrorist being able to communicate with their contacts
- Helping to prevent cyberspace from being used as a global platform for serious crimes, including the sexual abuse of children
- Keeping UK military aircraft safe from targeting by weapons systems

Recognising the importance of cyber to defence, in addition to the NCF last year the MoD created the 13th Signals Regiment, the first dedicated cyber regiment, and expanded the Defence Cyber School. These enhanced cyber capabilities bolster our defence and will play a vital part in operations including HMS Queen Elizabeth’s first global deployment this year. MoD cyber experts comprise almost half of the NCF’s cyber operators.

In addition to national security and defence applications, cyber technology can also be used to improve people’s lives through smart technology and helping people use the internet safely. In the last year, GCHQ has partnered with tech start-ups to help them develop and use AI to help train companies ensure more space for passengers during the COVID pandemic, alert haulage companies to stowaways in their containers and prevent the spread of misinformation online.

The Government’s new cyber strategy will support companies developing dual-use and consumer technology to ensure the UK is a cyber power in every sense.

It will also be critical to our ambition to establish the UK as a global services, digital and data hub.