National Cyber Force

A Defence and Intelligence Partnership

NATIONAL CYBER FORCE EXPLAINER

WHAT WE DO

The National Cyber Force (NCF) was established in 2020, a partnership between defence and intelligence, it is responsible for operating in and through cyberspace to disrupt, deny, degrade and contest those who would do harm to the UK and its allies, to keep the country safe and to protect and promote the UK's interests at home and abroad.

In addition to GCHQ and MOD, the Secret Intelligence Service and the Defence Science and Technology Laboratory are core partners, bringing cutting edge espionage and research techniques. It builds on the success of the National Offensive Cyber Programme and will transform the delivery of cyber operations, increasing their effectiveness and offering the opportunity to expand their capacity significantly. It has brought unity of command, integrating Defence and Intelligence capabilities and driving a more operational focus.

The publication of the Integrated Review of Security, Defence, Development and Foreign Policy has set the strategic direction for the UK's defence and security over the next ten years. The Review acknowledges the need for a whole of government approach to adapt to a more competitive and fluid international environment; to reinforce parts of the international architecture that are under threat; and to shape the international order of the future by working with others. The Review also recognises that cyberspace is becoming increasingly important in all areas of government and society, including defence, law enforcement and foreign policy. The IR makes it clear that the UK aims to maintain and cement its position as a top tier cyber power in order to sustain our competitive edge and to shape the norms and international order of a free, open, peaceful and secure cyberspace.

Through the launch of the National Cyber Strategy, HMG are taking a new, comprehensive approach to strengthening the UK's position as a responsible and democratic cyber power, able to protect and promote the UK's interests in and through cyberspace. The strategy takes a whole of cyber approach and the NCF is at the heart of this, providing the UK an ability to counter, disrupt, degrade and contest those who would do harm to the UK and its allies, to keep the country safe and to protect and promote the UK's interests.

The COVID-19 pandemic has demonstrated how reliant the UK is on cyberspace, to keep our society, economy and technology safe. This is significant given the existence of cyberspace makes it easier for our adversaries to perpetrate their activity at scale and across borders.

The UK has declared its willingness and ability to use cyber operations as an integral component of its diplomatic, economic and military activities. The NCF delivers a broad range of outcomes in the interests of national security, from the tactical through to the strategic, against state actors and non-state actors. Its work falls into three main categories:

1) Countering threats from terrorists, criminals and states who use the internet to operate across borders in order to do harm to the UK and other democratic societies.

2) Supporting the UK's cybersecurity and the work of the National Cyber Security Centre by countering threats which disrupt the confidentiality, integrity and availability of data and services in cyberspace.
3) Enabling UK Defence operations and helping deliver the UK's foreign policy agenda.

Governance

NCF operations are conducted in line with a well-established legal framework, which includes the Intelligence Services Act 1994, the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016. Operations conducted by NCF are subject to rigorous governance and are consistent with all UK and international law, including international humanitarian law when applicable. The Investigatory Powers Commissioner keeps the statutory powers used in the conduct of cyber operations under review. The Intelligence and Security Committee of Parliament also provides oversight of the NCF's activities. In contrast to some of our adversaries, the UK has previously made it clear that it will develop and deploy cyber capabilities responsibly, proportionately, and in accordance with UK and international law.

Accountability for NCF's activities is held jointly by the Secretary of State for Foreign, Commonwealth and Development Affairs, and the Secretary of State for Defence. NCF responds to priorities set by the National Security Council, and works closely with officials across several government departments to deliver outcomes in support of their strategies and campaign plans. Within the next few years NCF will establish its centre of gravity in the north west of England. It will contribute to driving growth in the technology, digital and defence sectors, and encourage the creation of partnerships between government, industry and universities in the region. This growth will allow us to enhance and broaden our collective skillset, deepening existing partnerships and forging new ones, strengthening the UK's cyber ecosystem.'