Heligan
Strategic Insights

Primer

An introduction to the National Cyber Force (NCF)

The National Cyber Force (NCF) recently celebrated its second anniversary. This HSI Primer aims to bring it out from the shadows and answer some key questions around what it is and what it does.

What is the NCF?

NCF was established in April 2020 and announced by the Prime Minister as part of the Integrated Review in November that year. It is the UK National Force charged with operating in cyberspace to disrupt, deny, degrade and contest those who would do harm to the UK and its allies…basically it is one of the National Security functions that keeps the country safe and protects and promotes the UK's interests at home and abroad.

The NCF was formed as a defence and intelligence partnership between GCHQ, MoD, MI6 and Dstl, drawing together personnel from each organisation…and Heligan believes it's definitely one of those partnerships that is more than the sum of its parts.

NCF is headquartered in a new facility (within an existing site owned and operated by BAE Systems) in Samlesbury, south Lancashire, on the outskirts of Preston.

The NCF is built on the foundations and success of the National Offensive Cyber Programme (NOC-P) that was run out of GCHQ for many years and has transformed the delivery of cyber operations in the UK. It has brought a unity of command, integrating Defence and Intelligence capabilities in this new area of operations - cyberspace.

Primer

What does the NCF do?

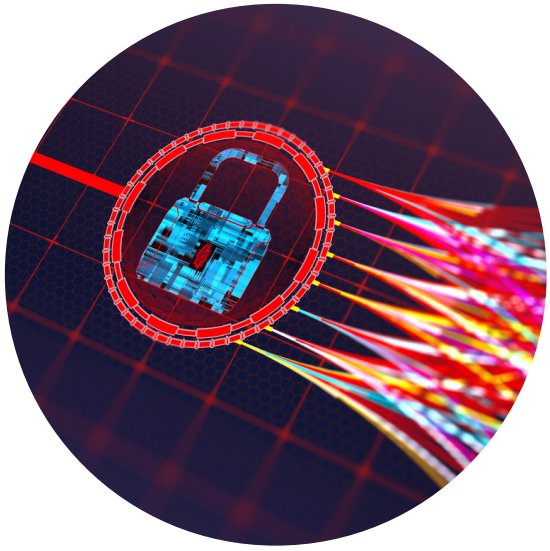
With the establishment of the NCF, the UK has stated its willingness and ability to use cyber operations as an key component of its diplomatic, economic and military activities. The NCF delivers a broad range of outcomes in the interests of national security, from the tactical through to the strategic, 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 - This means it is actively looking for adversaries that are out there trying to carry out cyber attacks on the UK and using our own cyber attacks on them to stop them in their tracks.

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 - Helping the NCSC identify illegal online activities and then disrupting the disruptors before they can launch attacks like Distributed Denial of Service Attacks (DDOS) or Phishing attacks.

3. Enabling UK Defence operations and helping deliver the UK's foreign policy agenda - In contrast to some of our adversaries, the UK has made it clear that it will develop and deploy cyber capabilities responsibly, proportionately, and in accordance with UK and international law.

Details of the NCF budget are not easy to come by due to the nature of the way it is funded through different Government departments and agencies. Accountability for NCF's activities is held jointly by the Secretary of State for Foreign, Commonwealth and Development Affairs (FCDO), and the Secretary of State for Defence. The Intelligence and Security Committee (ISC) also provides oversight of the NCF's activities and the NCF also responds to priorities set by the National Security Council.



In short there are a lot of competing asks which Heligan assesses will need to be ironed out over the coming years as the NCF matures and finds their place in the wider NS community as an independent player...as they surely will.