# Britain pledges £1 billion to launch offensive cyber command targeting Russia and other threats



Britain is set to launch a substantial initiative aimed at boosting its cyber warfare capabilities, with the government pledging £1 billion to establish an expansive cyber force targeted primarily at adversaries like Russia. Defence Secretary John Healey outlined the government's ambitious plan, which includes forming a cyber command to mitigate a surge in cyber warfare that he described as "continual and intensifying." This strategic move comes amid increasing concerns about the number of cyber attacks, with reports indicating approximately 90,000 incidents linked to state-sponsored actors have been directed at the UK's defence in just the past two years.

The planned cyber command will not only bolster defensive strategies but also enhance offensive capabilities. According to the Ministry of Defence, the initiative aims to create a "digital targeting web" by 2027, which will enable better integration of various military systems. This system is envisioned to rapidly detect threats—utilising sensors from naval vessels or satellite systems—and respond effectively through advanced platforms such as F-35 fighters, drones, or cyber operations. Healey remarked during a visit to the Ministry of Defence in Corsham that the intense cyber threats necessitate a robust enhancement of national defence capabilities.

Britain's evolving cyber strategy aligns with broader international security objectives, as outlined in its National Cyber Strategy 2022. This strategy includes plans to consolidate various cyber operations under the newly formed Cyber and Electromagnetic Command. This restructured entity will take charge of both defensive measures and offensive cyber manoeuvres, facilitating coordinated responses to threats posed by state actors such as Russia, China, and North Korea. The National Cyber Force, long engaged in counter-terrorism and other security measures, will collaborate with the new command to disrupt adversaries' cyber capabilities and operations.

The current push towards offensive cyber capabilities isn't merely a reaction to immediate threats; it reflects a growing recognition that modern conflicts increasingly play out in the digital realm. Philip Hammond, former Chancellor, previously underscored the necessity for the UK to enhance its offensive capabilities to deter nations from aggressive cyber actions, highlighting the potential consequences of adopting a passive stance.

Furthermore, this initiative is supported by recent government investments in global security, which include significant funding for enhancing cyber security initiatives across multiple regions. For example, £25.5 million has been earmarked specifically for cyber programmes in countries like Ukraine and Iraq, intending to fortify their own defences against cyber threats while simultaneously addressing the international dimensions of cyber security.

As Britain steps up its cyber capabilities, the implications for global security dynamics are profound. The establishment of an enhanced cyber command and the strategic emphasis on offensive operations signify a shift in how the UK approaches both defence and deterrence in an age where cyber warfare is a critical component of national security. This proactive stance will not only aim to protect the UK's critical national infrastructure but will also position it as a formidable player on the international cyber battlefield.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14759625/Britain-set-splash-1billion-army-hackers-target-likes-Putin.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.gov.uk/government/news/huge-boost-for-global-security-with-almost-1-billion-government-investment)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/news/article-14759625/Britain-set-splash-1billion-army-hackers-target-likes-Putin.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[3]](https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022), [[4]](https://www.theguardian.com/technology/2023/apr/03/uks-offensive-hacking-unit-takes-on-military-opponents-and-terrorist-groups)
* Paragraph 3 – [[6]](https://www.itpro.com/security/27501/uk-needs-to-develop-offensive-cyber-capabilities-says-hammond), [[5]](https://www.army-technology.com/features/from-defensive-to-offensive-the-uk-boosts-its-cyber-units/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14759625/Britain-set-splash-1billion-army-hackers-target-likes-Putin.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.gov.uk/government/news/huge-boost-for-global-security-with-almost-1-billion-government-investment> - In January 2024, the UK government announced an investment of £830 million in the 2022 to 2023 financial year to support global security initiatives. This funding was allocated to various programmes and peacekeeping efforts across more than 90 countries, including Ukraine, Africa, the Indo-Pacific, and the Overseas Territories. Notably, the government increased spending on cyber security programmes, dedicating £25.5 million to the Global Cyber Programme, the Africa Joint Operations Against Cyber Crime, and enhancing cyber defences in countries like Georgia and Iraq.
3. <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022> - The UK's National Cyber Strategy 2022 outlines objectives to bolster the nation's cyber capabilities by 2025. A key goal is to scale up and develop the National Cyber Force (NCF), integrating it with agencies such as GCHQ, the Ministry of Defence (MOD), the Secret Intelligence Service (SIS/MI6), and the Defence Science and Technology Laboratory (DSTL). The strategy emphasises delivering legal and proportionate offensive cyber operations through the NCF to support national security priorities, including defence, foreign policy, and the prevention of serious crime.
4. <https://www.theguardian.com/technology/2023/apr/03/uks-offensive-hacking-unit-takes-on-military-opponents-and-terrorist-groups> - In April 2023, the UK's National Cyber Force (NCF) issued its first policy statement, detailing its daily operations to disrupt terrorist groups, combat child sexual abuse material distribution, and counter military opponents. The NCF employs techniques to undermine the tradecraft of state-sponsored hackers from nations like Russia and China. Its activities include technical disruption against terrorist groups to prevent the spread of online propaganda and supporting military operations by degrading adversaries' cyber capabilities.
5. <https://www.army-technology.com/features/from-defensive-to-offensive-the-uk-boosts-its-cyber-units/> - In May 2023, Defence Secretary Penny Mordaunt announced a £22 million funding commitment for the British Army to establish new cyber operations centres across the UK. These centres aim to integrate cyber capabilities from national intelligence and open-source data to provide the army with a competitive edge in all environments. The initiative is part of a broader £1.9 billion investment in the UK's National Cyber Security Strategy, which includes the creation of the National Cyber Security Centre (NCSC) and the development of military-focused cyber capabilities by the MOD.
6. <https://www.itpro.com/security/27501/uk-needs-to-develop-offensive-cyber-capabilities-says-hammond> - In 2014, UK Chancellor Philip Hammond emphasised the necessity for the UK to develop offensive cyber capabilities to respond to nation-state cyber attacks. He highlighted that without such capabilities, the UK would be forced to either remain passive or respond with military force in the event of an attack. Hammond's comments underscored the importance of building a cyber strike capability to deter adversaries and protect critical national infrastructure from cyber threats.
7. <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022> - The UK's National Cyber Strategy 2022 outlines objectives to bolster the nation's cyber capabilities by 2025. A key goal is to scale up and develop the National Cyber Force (NCF), integrating it with agencies such as GCHQ, the Ministry of Defence (MOD), the Secret Intelligence Service (SIS/MI6), and the Defence Science and Technology Laboratory (DSTL). The strategy emphasises delivering legal and proportionate offensive cyber operations through the NCF to support national security priorities, including defence, foreign policy, and the prevention of serious crime.