

Press release: Cyber innovation at the forefront of UK's approach to modern warfare

Speaking this evening at the NATO Cyber Defence Pledge Conference in London, Defence Secretary Penny Mordaunt will address the need for the UK and NATO members to recognise offensive cyber as central to modern warfare. As the UK has already demonstrated against Daesh in the Middle East, it can be a vital tool to keep people in the UK and overseas safe from virtual and physical threats.

The military continues to develop its cyber capabilities as part of the £1.9 billion investment into the National Cyber Security Strategy, focused on boosting the UK's cyber security. Recent UK innovations have included the creation of the National Cyber Security Centre which brings together government, intelligence agencies and the private sector into one organisation. The state-of-the-art Defence Cyber School, which marked its first anniversary in March this year, is also training the next generation of cyber experts.

The Defence Secretary will today expand that commitment, announcing £22 million in funding to stand up new Army cyber operations centres across the UK.

Defence Secretary Penny Mordaunt will say:

We know all about the dangers. Whether the attacks come from Russia, China or North Korea. Whether they come from hacktivists, criminals or extremists. Whether its malware or fake news. Cyber can bring down our national infrastructure and undermine our democracy.

It's time to pay more than lip service to cyber. We must convince our adversaries their advances simply aren't worth the cost. Cyber enemies think they can act with impunity. We must show them they can't. That we are ready to respond at a time and place of our choosing in any domain, not just the virtual world.

We need coherent cyber offense as well as defence. So today I can announce we will be investing £22m to create new cyber operations centres.

Putting the Army at the forefront of information warfare, the centres will draw together cyber capability from a range of sources – including both national intelligence and open source data – to give the Army the competitive edge across all environments.

The cyber centres will provide the Army with 24/7 information and analysis, dispel misinformation and give the UK Armed Forces and our allies the upper hand on emerging digital threats. The centres are likely to be used to support overseas operations, humanitarian missions, and efforts to protect UK digital communications on home soil.

The centres will work with existing Army capabilities, such as 77 Brigade – a modern and information-focused British Army unit – but will also have regular contact with joint and other national security organisations.

Major General Tom Copinger-Symes, General Officer Commanding Force Troops Command:

These new cyber centres will allow the Army and Defence to transform the way we use data, at speed, so that we can compete with our adversaries in a way fit for the 21st Century.

Combining artificial intelligence with our military analysts will help us better understand threats and exploit opportunities, in turn enabling us to get the truth out much more rapidly, quashing the noise of disinformation from our enemies.

While details on locations are yet to be confirmed, building in support of the centres is due to begin next year, with operations expected to commence in the early 2020s.

The MOD is embracing transformation at an ever-faster rate and investments in truly high-tech innovation, such as in the provision of cutting-edge cyber centres, that will develop the Armed Forces of the future.