Written evidence submitted by the Ministry of Defence

At the oral evidence session on 30th June, I undertook to provide the House of Commons Defence Committee with an update on NATO's progress in the cyber domain.

Cyber brings additional complexities to the structure and processes of NATO and our allies. As a leading nation in NATO on cyber, the UK has been working to ensure that NATO secures its own networks and encouraging all partners to develop their own cyber capabilities.[1]

NATO has been strengthening its cyber capabilities since the requirement was first acknowledged by Allies at the Prague Summit in 2002. The Alliance's approach to cyber has become considerably more mature since the adoption of the 2014 Enhanced NATO Policy on Cyber Defence and its associated action plans. The Alliance agreed, in 2016, to recognise cyberspace as an operational domain at the Warsaw Summit, in alignment with UK doctrine.

Notable progress has been made in many areas:

- NATO military authorities have sought to integrate cyber into a cross-domain approach. This recognises that operations in cyberspace may support conventional military activity, and vice versa, or that activity may remain within the domain altogether.

- Secretary General Jens Stoltenberg has unambiguously stated that "a serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all"[2]. The determining factor would be whether an incident is considered to have met the threshold of an armed attack. Whilst this is not prescriptively described in international law nor the North Atlantic Treaty, an Ally may request to invoke Article 5 in response to an unconventional attack using unconventional weapons – including a cyber-attack.

- In February 2019, NATO defence ministers endorsed a NATO guide that sets out a number of tools to further strengthen NATO's ability to respond to significant malicious cyber activities. NATO needs to use all the tools at its disposal, including political, diplomatic and military, to tackle the cyber threats that it faces. The response options outlined in the NATO guide will help NATO and its Allies to enhance their situational awareness about what

[1] Cyber Primer, 2nd Ed

[2] https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

is happening in cyberspace, boost their resilience, and work together with partners to deter, defend against and counter the full spectrum of cyber threats.

- A new Cyberspace Operations Centre in Mons, Belgium, provides military commanders with situational awareness and ability to coordinate NATO operational activity in cyberspace.

- Allies have agreed on the principles to support the integration of sovereign cyber capabilities provided on a voluntary basis to Alliance operations and missions. In addition, cyber defence capability targets are included in the NATO Defence Planning Process, providing coordination in the development of, and more effective integration of, Allies' national defensive capabilities.

- In line with their Cyber Defence Pledge, Allies have been committed since 2016 to strengthening and enhancing the cyber defences of their national infrastructures and networks as a matter of priority – including systems upon which NATO depends. This commitment was reaffirmed during the second conference on the Pledge in London in May 2019. NATO has given particular initial attention to training & education, and cyber risk to military supply chains.

- Further commitments have been made to improve lines of communication between Allies' defensive cyber actors, invest in cyber skills and awareness, and to training and exercising. Defence Ministers agreed revised baseline requirement for resilient communication systems in 2019 in anticipation of the challenges presented by emerging technologies.

- NATO engagement with partner countries, international and regional organisations and industry has grown in depth and breadth. Cyber defence features in a significant number of partnership programmes as an area for cooperation. And partners have been invited to observe and participate in NATO cyber exercises.

The Alliance's achievements and continued efforts to strengthen its cyber capabilities and defence ensure that the it will be fit and ready to respond to cyber threats and operate in cyberspace.

THE RT HON BEN WALLACE MP
21 July 2020