



THE CABINET OFFICE
LONDON SW1A 2AS

From The National Security Adviser

Dame Margaret Beckett DBE MP
Chair
JCNSS
C/O House of Commons

Thursday 10 March 2016

Dear Chair,

During my appearance before the Joint Committee on the National Security Strategy on 1 February 2016, I promised further information on four issues: whether the National Security Secretariat would provide a confidential briefing on the NSS and the NSRA (Q47 & 53); whether there was a definition of an energy problem that was so important that it became a security issue (Q56-64); how many people have been recruited to deal with the cyber skills shortage (Q68); and further detail on cooperation with companies providing communications services to users in the UK (Q70).

a) Confidential briefings on the National Security Strategy and the National Security Risk Assessment (Q47 & 53)

Senior Officials from the National Security Secretariat, including myself, would be happy to provide a briefing in confidence to the Committee before the end of April. My team is in touch with the Committee clerks to arrange dates.

b) Whether there is a definition of a problem in energy that is so important that it moves out of the normal commercial sphere and goes into security (Q56-64)?

The UK energy sector operates within a legal and regulatory framework designed to ensure safety and security and that risks are effectively managed. For example, the Energy Act 2013 created the Office of Nuclear Regulation, which, as an independent regulator, has specific responsibilities for safety and

security in the civil nuclear sector. The Government continues to take an overview of any risks to national energy infrastructure to ensure that these risks are being effectively managed. The Government welcomes any foreign investment that meets our high regulatory and legal standards. If any national security concerns arise, the Government will assess those risks and put in place mitigation to provide greater certainty for investors. There is no fixed definition of a national security concern as part of this; it is considered on a case-by-case basis taking into account whether the investment would constitute a change of ownership that could pose national security risks, including to the UK's critical national infrastructure or the safety of British citizens.

c) How many people have been recruited to deal with the cyber skills shortage (Q68).

The National Cyber Security Programme has funded interventions at every level of the education system, in order that students pursuing a cyber security career can progress beyond Key Stage 3-postgraduate level (providing vocational & academic entry routes). As a recognised centre of expertise in cyber security, GCHQ's work in education and skills has focused on meeting its own and security and intelligence agency needs, as well as those of the wider economy, creating a pipeline of entry points. In 2012, GCHQ launched its cyber apprenticeship scheme to complement its existing graduate recruitment programme, and support the security and intelligence agencies. Those that complete the course are expected to stay with the agencies for a minimum of 2 years. The CyberFirst scheme was launched in March 2015 with 20 students and is intended to identify exceptional talent from the broadest range of backgrounds, that can be developed and nurtured to support the UK's future national security needs in cyber space. Its aim is to increase the number of outstanding students following a career in cyber security by providing financial assistance, work experience, and then guaranteed employment on graduation. The pilot programme of 20 has been successful. By the end of 2020, the intent is to expand the programme to 1000 students.

The search for talent must begin as early as possible. Following a pilot last year, in 2016 GCHQ will run a series of summer camps to introduce Year 12 and Year 13 students to cyber security. It will continue to work with national competitions to identify aptitude, as well as working closely with initiatives such as the Cyber Security Challenge Schools Programme, Cyber Centurion, and the forthcoming National Cyber Schools Programme. This will raise awareness of cyber security to the broadest community and build the pipeline of talent entering the profession within the security and intelligence agencies and beyond.

d) Cooperation with companies providing communications services to users in the UK (Q70)

The Government's Investigatory Powers Bill will ensure that the UK's law enforcement and intelligence agencies continue to have the powers they need to keep the public safe. The Bill makes clear the obligations on companies providing communications services to users in the UK to comply with UK warrants requesting the content of criminal and terrorist communications, and with notices requiring the disclosure of communications data. As the Prime Minister and Home Secretary have previously stated, the Government is also engaging in preliminary discussions with international partners on how a new framework for access to data across jurisdictions might operate. This would be based on strong, human rights-compliant domestic regulatory oversight. The Government has also appointed an Envoy to the US Communication Service Providers, Antonia Romeo, whose role is to build and maintain constructive relationships across the range of Government work; on security, growth, investment, tax and regulation.

Yours

MARK LYALL GRANT