On Thursday, February 20th, 2020 the AEJ held a lunchtime meeting with Nicola Hudson, Director of Policy and Communications at the National Cyber Security Centre (NCSC). The venue was Herringham Hall at Regent's University London.

By Peter Norman

For the 30 or so journalists and a dozen Regent's University students present the AEJ's meeting with Nicola Hudson yielded fascinating insights into the work and purpose of the UK's National Cyber Security Centre (NCSC), the still young and relatively little-known government organisation tasked with: "Making the UK the safest place to live and work online."

Established in 2016, the NCSC functions in two very different worlds. It is an operational division of GCHQ, the UK's signals intelligence agency, and as such it participated in discussions that led to the government's recent controversial decision to allow the Chinese company Huawei limited involvement in the development of 5G mobile telecommunications in Britain. At the same time the NCSC is seeking ways of making the UK public and crucial sectors of the economy and society more aware of fast growing cyber threats while also devising innovative ways of building up the population's cyber security skills for a future in which artificial intelligence, computer power and online activity will be ever more central.

Nicola Hudson joined the NCSC in September 2016, having been head of news in the office of Prime Minister David Cameron. The NCSC describes her present role as "leading on all aspects of Cyber Policy and Strategic and External Communications". In her opening on-the-record remarks to the AEJ, she focused on the NCSC's work to protect, prepare and educate the UK against cyber threats. A discussion which followed her initial remarks took place on a deep background basis and forms no part of this summary.

The NCSC was established by pooling the cyber security skills of several government departments and the UK intelligence agencies after Prime Minister Cameron and George Osborne, his Chancellor of the Exchequer, determined that the UK government needed a substantial and coordinated response to growing cyber threats. In aiming to make the UK the safest place to live and work online, the NCSC deals with incidents and works to understand threats and to prevent serious incidents from happening.

Ms Hudson said the NCSC has defined six categories of threat. Category 6,5 and 4 threats are "triaged" as low impact and handled by other agencies. Threats in categories 3,2 and 1 are dealt with by the NCSC. She disclosed that the NCSC had dealt with 2,000 category 3 or 2 threats, citing the 2017 WannaCry ransomware attack as category 2. The UK has so far not experienced a category 1 attack, defined as one which would have a massive and catastrophic impact. Once faced with such an incident, the NCSC's task is to assess the threat, its impact and how to mitigate its effects.

In understanding cyber threats, the NCSC's first task is to locate where a threat comes from. Four countries -- Russia, Iran, North Korea and China -- pose "very different threats" to the UK. There is also a growing cyber criminal element which is a "massive part of the threat" facing the country. Cyber threats are becoming "commoditised" and easier and cheaper to launch.

To combat these trends the NCSC has to understand the threats and share information, especially on threat mitigation, widely with those at risk, be they businesses or the general public. The agency has formed online "trust groups" to get information out to certain

businesses. It also has "engagement teams" to keep specific sectors of society up to speed on threats and developments.

Different teams, with tailored messages, target different sectors ranging from critical national infrastructures, such as waterworks, power stations and railways, through central and local government departments to law firms, charitable organisations and sporting groups. Such initiatives form part of an "active cyber defence programme" in which technical experts produce solutions to help people protect themselves.

A significant problem is getting the cyber security message through to the general public. Ms Hudson noted that there is a general perception among the public that people can't do anything much to avoid cyber crime. The NCSC, with the Home Office and the help of behavioural scientists, is developing a campaign to tell the public how to protect themselves, notably by teaching people how to devise easy to remember but secure passwords. An important part of the campaign, due for launch in May, will be teaching people to pay special attention to passwords for important "gateway" services such email which often open the way for criminals to access other online activities involving money, such as shopping and banking.

Another important part of the NCSC's work is raising the UK's cyber skills - and especially those of young people -- on a "pathway" to enable the UK to cope with whatever threats emerge in the years to come. In January 12,000 12 to 13 year old girls took part in an online cyber competition that involved solving hundreds of computer puzzles. The focus on girls in this case was part of a programme of diversity and inclusion. To raise the UK's cyber skills base for the future the NCSC also organises weekend courses for teenagers, week long training for 17-18 year olds and cyber security partnerships with universities.

Summing up, Nicola Hudson emphasised that the NCSC is still a very new organisation. Work is still in progress on an updated government cyber strategy. Due next year, this will underline the importance of government working with industry and other interested parties as part of a wider support system to make the UK a safer place to work and socialise online. An important goal, she said, will be to give people trust in cyber space as this will be "a basic part of life going forward". Achieving this goal will involve giving due deference to cyber security, through its incorporation in legislation and regulation and putting it "at the heart of things" in the future.