Speech: Chancellor of the Duchy of Lancaster speech to Women in Security Network: 18 June 2019

Hello, and thank you for having me here today. In the four years since it was created, the Women in Security Network has provided a crucial forum for women and underrepresented groups to gain skills and connections to help them get ahead in their careers.

We all agree that the national security profession should reflect those it works to protect. So I am delighted to speak today about some of the work this Government is undertaking through the National Cyber Security Strategy to ensure a vibrant and representative cyber security profession.

Of course, women have served in security and technology throughout history – and have often been pioneers in computing and codebreaking. I've attended briefings in the Lovelace Room, right here in the National Cyber Security Centre. Each briefing in that room is an excellent reminder how women such as Ada Lovelace, Joan Clark, and Mavis Batey have been trailblazers in this field. But women need to be the rule and not the exception – especially when it comes to cyber security.

Today, cyber security is among the most important aspects of our national defence as we work to protect the UK and the British people.

The National Cyber Security Strategy has revolutionised the UK's fight against cyber threats as an ambitious, deliberately interventionist programme of action. During the last three years, we have put in place many of the building blocks to strengthen our cyber security and resilience, backed by an investment of £1.9 billion pounds.

In 2016, we set up the world-leading National Cyber Security Centre to act as our single authority on cyber security. We've invested in cutting-edge cyber capabilities across all tiers of UK Law Enforcement. And we're protecting UK internet users from lower-sophistication, high-volume attacks that have an impact on people's everyday lives, that compromise their identities and undermine the individual security of their bank accounts.

More than halfway into the Strategy, we're seeing behavioural changes, too – and not just from our warnings to an estimated 23 million account holders that 123456 isn't a suitable password! In Government and in the private sector, we're also seeing Boards integrate cyber security into the core functions of their organisations. The results of DCMS's Cyber Security Breaches Survey 2019 make clear that cyber security is increasingly a key issue for organisations, with three quarters of business and charities now rating it as a high priority. So we've made considerable progress in Government, and with industry. And the people in this building have been a crucial part of that success.

But, we also recognise that there is much more work to be done.

The government, and indeed, the national security profession – must reflect those that it seeks to represent and protect. Yet, national security has the lowest representation of women than any other profession in Government, at 15.7 percent. And the National Security Council Officials board has the lowest proportion of female officials than any other Civil Service board.

The British government isn't alone. There remains a severe lack of diversity and representation in the cyber security industry. According to a report from the Global Information Security Workforce, only 11% of the global workforce is made up of women – this falls to a mere 7% elsewhere in Europe.

And we've seen the risks in other sectors when technology doesn't get diversity right. A New York Times piece published yesterday outlined how human biases in artificial intelligence technology have led to minorities and underrepresented groups being turned down for job opportunities, denied bank loans and even misidentified as criminals. Because when the faces who create AI systems are all male, or white, the algorithms are unable to recognise other groups as easily.

At the same time, we've seen ample research on how more diverse organisations do better at meeting their objectives. McKinsey studies of the British private sector show that greater gender diversity at the senior level corresponds to higher performance. So there is a business imperative, as well as a moral one.

There are lots of ways to address the issue of diversity. But today, I'm going to focus on the urgency of addressing the skills gap in cyber security, and the importance of cultivating the right workplace environment.

Cyber security is a nascent profession, which provides us with a narrow opportunity to shape its future. We need to be inspiring the next generation to think about a career in this field. There is a wealth of talented young people across the UK who could have successful careers in cyber security. Teenagers who are livestreamers with their own gaming vlogs. Students who consider Twitter their second language. They do not need to be fluent in Javascript to be the future of the industry.

Many of you in this room have been involved in valuable efforts to engage younger people – especially young girls – in cyber security. In 2015, GCHQ launched the CyberFirst programme to give talented young people the support, skills, experience and exposure they need to become 'cyberists' of the future.

This year, nearly 12,000 talented 12-13 year-old female students from over 800 schools across the UK took part in the CyberFirst Girls Competition. Last year, 44% of CyberFirst attendees were female. And in the Cyber Skills programme, female participation is at 23%, with the aim of achieving gender balance.

At the same time, we also recognise that financial barriers can prevent very capable people from pursuing their chosen path. So the CyberFirst University Bursary aims to remove these barriers and give young people access to the training and skills they need to succeed, regardless of background. These are vital steps in unlocking and opening up the profession to young people, and I commend them wholeheartedly.

However, it is important that senior leaders recognise that an emphasis on skills-building isn’t the only piece of the puzzle. There needs to be a cultural shift in the way we think about gender equality and diversity. We need to ensure that we don’t treat this as a tick-box exercise, thinking that the job is done once the recruitment process has been finalised. Instead, we all need to be thinking about the broader, collective environment we create for new recruits. That means replicating opportunities for mentorship, like the network that you have so successfully built here. But it also means encouraging more senior male leaders to mentor women and improve the underlying culture, as recommended by Harvard Business Review.

Of course, a commitment to diversity is something even more rudimentary than skills, initiatives, or pathways. It means empowering staff to pursue their careers, building the confidence to constructively challenge their environments, and ensuring that they can construct opportunities for their colleagues in the future. This is the sort of power that diversity can bring to a profession as young and as pioneering as cyber security, and I challenge you all to embed this across your teams.

When a young Ada Lovelace began her mathematical studies, her tutor fretted that “the very great tension of mind [that mathematics] require is beyond the strength of a woman’s physical power of application.” Ada, of course, went on to become a visionary of computer programming. And we can now laugh at this outdated thinking.

But subtler societal perceptions persist. We can, and must, do more to encourage that a more diverse body of talent is represented at every level of government, business and beyond. Because as we chart the course for cyber security, we must ensure that our aims for the future of this profession remain as ambitious as our algorithms.

And now, your questions.

[Checked against delivery].