Speech: Defence Secretary's speech at Cyber 2017 Chatham House Conference

Good afternoon, and thank you again to Chatham House for putting on this very timely event at a timely moment. Last Friday we saw the United Kingdom hit by yet another cyber attack, this time directed against our Parliamentary IT facilities.

Investigations so far have found that the hackers were attempting to carry out a sustained and determined attack on all parliamentary user accounts in an attempt to identify weak passwords and to gain access to users' emails.

Immediate steps have been taken to address that particular problem.

It has meant that some Members of Parliament and staff have been temporarily unable to access their email accounts outside of Westminster.

As MPs, some have been unable to answer constituents' emails on a Sunday, and we've had to live with that.

Since then, the National Cyber Security Centre has been working around the clock with our UK Parliamentary Digital service to understand the nature of the attack, to contain it, and to put in place mitigation measures to prevent possible future breaches.

Now, this latest attack is far away from being an isolated incident. It follows hot on the heels of the Wannacry virus that didn't just shut down NHS operating theatres, but in the end affected more than 200,000 people over 150 different countries. So here was yet more evidence that cyber is a truly global phenomenon, evidence that has been piling up following the attacks on Germany's lower house of Parliament.

Bulgaria has also suffered, and I quote from them, according to their President, "the heaviest and most intense cyber attack…conducted in south-east Europe." And of course, there have been attacks on America, with the United States Office of the Director of National Intelligence concluding that Russia had targeted the Presidential election.

I quote, its "intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties."

All these attacks point to our adversaries becoming more diverse, becoming better at what they do, and becoming more adept at using virtual attacks to inflict very real damage. One in five British businesses has been hacked by cyber criminals in the last year according to the British Chambers of Commerce. Analysts put the cost to our economy already in the billions, while it's been estimated that the United States lose up to 3 per cent of GDP to Intellectual Property theft.

For the military, the consequences of cyber disruption are equally devastating. Reuters has reported that Russia used malware implants on Android devices to track and target Ukrainian artillery. That's why back in the 2015 Strategic Defence and Security Review we put cyber up there with terror and major natural hazards as a Tier One threat to this country. To date, alarming as some these attacks have been, our people have proved equal to the task of defending against them. Fewer than 1 per cent of the 9,000 email accounts on the parliamentary network were compromised. But there is absolutely no complacency here.

We are investing a huge chunk of money – some £1.9bn – into boosting our cyber security And Defence, in particular, has a three-fold role to play in this national cyber security effort.

Keeping our house in order

First and foremost, we're keeping our digital house in order. We're not just working closely with the National Cyber Security Centre to ensure that our military and civilian systems are robust.

We have networks of information risk and asset owners embedded in our organisation to properly police data and to deal with problems.

And we are encouraging all our staff to observe good cyber etiquette.

They must now complete mandatory information handling refresher training annually and they must take personal responsibility for their data.

We're also doing more to recruit the cyber savvy. There's our cyber reservists, experts from industry and academia who are putting their high tech skills at the service of the nation by weeding out network vulnerabilities. At the same time, we're building up a new 21stcentury Cyber Corps, a band of expert volunteers, leaders in industry, who are going advise us on how to keep ahead in the cyber space race. Finally, cyber is becoming now a core part of our military training. In January, we will open a dedicated state-of-the-art Defence Cyber School at Shrivenham, bringing together all our military joint cyber training into one place. And we look forward to that first class of 2018 emerging with the digital X-factor to transform our future cyber capability.

Creating a culture of resilience

Second, the interconnected nature of the web, the way it blurs the boundaries between military and civilian, between public and private, means we all have a responsibility to look after ourselves online.

A stronger password here, a Windows update there, and we would have stood an even better chance of warding off the Parliamentary and Wannacry attacks. So my second point is that the MOD has a key role to play in contributing to a culture of resilience. That's why we set up the Defence Cyber Partnership Programme (DCPP) to ensure that companies with whom we have defence contracts are properly protecting themselves and meeting a host of cyber

security standards.

Strengthening our deterrence

But there's a third way in which we can protect our national infrastructure, and that's by strengthening our deterrence. So we're using our rising budget to invest our £178bn in full spectrum capability, from carriers to Ajax armoured vehicles, fifth generation F35 to the latest UAVs, signalling to potential cyber strikers that the price of an online attack could invite a response from any domain, air, land, sea or cyber space. And when it comes to the latter, we're making sure that offensive cyber is now an integral part of our arsenal. We now have the skills to expose cyber criminals, to them hunt down and to prosecute them, to respond in kind to any assault at a time of our choosing.

Our National Offensive Cyber Planning allows us to integrate cyber into all our military operations. And I can confirm that we are now using offensive cyber routinely in the war against Daesh, not only in Iraq but also in the campaign to liberate Raqqa and other towns on the Euphrates. Offensive cyber there is already beginning to have a major effect on degrading Daesh's capabilities.

We're determined as a coalition to maintain our advantage in this arena and that is why we are investing with our allies in the sort of kit capable of data use.

To help create a picture of the virtual battlefield we have recently here in the United Kingdom launched a multimillion pound competition to develop machine learning algorithms and Artificial Intelligence which will assimilate this wealth of new data and will free up our personnel to deliver a more coordinated, targeted response. The first contracts from that investment have already been awarded to a variety of UK suppliers including from academia and innovative micro-scale businesses and other SMEs, all of whom are working on a range of solutions from rapid sensor integration to predictive cognitive control systems.

International partnerships

Cyber deterrence is obviously stronger when we stand together with our like-minded allies. And that's why we're working hard, in particular, to get NATO, the bedrock of our security, to do more to defend effectively online.

At last year's Warsaw summit we achieved a breakthrough in getting the Alliance to recognise cyber as a distinctive domain of operations. We also succeeded in persuading NATO nations to sign the cyber pledge, committing Allies to enhance their national defences as a priority and to strengthen their capability, collectively and individually, to resist cyber attacks in any form. There remains work to be done to share our data to deal with major incidents together and to improve the underlying infrastructure of the Internet. At the same time, we will also need new doctrine to clarify our response within NATO to anonymous cyber activity which often takes place now in that grey zone below the previously understood threshold of war.

And all the while we are developing the effects, covert and overt, cognitive and physical, to help provide a proportionate response to those cyber attacks.

But Alliance effectiveness in the virtual world would be immeasurably enhanced if national capabilities were made ready to deploy in support of NATO operations. So having honed our own UK pioneering cyber techniques against Daesh in Iraq and Syria, I can confirm today that United Kingdom is ready to become one of the first NATO members to publicly offer such support to NATO operations as and when required. ### Conclusion

So let me say in conclusion that cyber is a serious problem. It is a growing problem. But my message to you is that Government here and Defence, in particular, is on the case. Over the next few years we're going to be redoubling our efforts to strengthen our resilience against our adversaries, to strengthen our hand against our cyber adversaries and to ensure those who mean to do our country harm, offline or online, have nowhere to hide.