EMBARGOED UNTIL 0001 WED 13 OCT 2010
Check against delivery

DIRECTOR GCHQ CYBER SPEECH FOR INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES TUESDAY 12 OCTOBER

My staff tried to persuade me to begin with 'unaccustomed as I am to public speaking'. I think you would all recognise that this is an unusual step for a serving GCHQ Director to take. But I feel that the increasing public interest in Cyber calls for some attributable comments on GCHQ's perspective.

My colleague Jonathan Evans referred to the growing priority of Cyber Security in his speech last month to the Worshipful Company of Security Professionals. You might consider these remarks as a follow-up to that reference.

But first a few words on the organisation that I lead, and why I believe it is important to understand its

contribution to the UK's response to the Cyber challenge, within the broader national security framework.

GCHQ is probably best known for its foreign intelligence mission, providing Signals Intelligence or 'Sigint'. Its current contributions support a wide range of national security activity including:

- support to the military in Afghanistan and more broadly;
- counter-terrorism, supporting Security Service investigations and working with the Secret Intelligence Service to understand the upstream threat;
- counter-proliferation;
- tackling serious and organised crime;
- and a range of other global security issues.

All of this takes place under close Ministerial oversight and appropriate authorisation by the Secretary of State. There

is judicial oversight from the Intelligence Services and Interception Commissioners. Parliamentary oversight comes through the Intelligence and Security Committee.

But it is perhaps not so widely known that GCHQ also has a clear security mission. The precise description is “to provide advice and assistance about... cryptography and other matters relating to the protection of information and other material”. Within Government we describe that more simply as the “Information Assurance” mission.

Both of these missions have a proud history - you’re all aware of course of the origins of GCHQ in Bletchley Park’s successes in code-breaking and code-making and the remarkable technology and people that delivered them. Through the intervening years our achievements have remained at that high level of technological

expertise. Our people, of whom I am immensely proud, remain one of this country's great unsung assets.

Our mastery of high-end communications technology is hugely relevant to the problems of Cyber Security, as I hope I shall demonstrate this evening. You may have noticed that although we still keep very quiet about our operational successes there has been a bit more by way of on-the-record comment from GCHQ recently. I think that's important. One significant change that's taken place in international communications is that in the modern world the same technology that our adversaries use is used by citizens going about their daily business. So reassuring people that they are being appropriately defended against threats without encroachments on their privacy is very important. I also want to bang the drum publicly about the importance of technology and Cyber skills so that we can sustain a flow of top-quality recruits into GCHQ and its industry partners.

My perspective on Cyber comes from bringing together both sides of GCHQ's mission:

- the intelligence mission illuminates some of the capabilities - and sometimes the intentions of adversaries to use Cyber techniques. It allows us to detect some of their activities.
- And the information assurance mission gives us knowledge of where our own government and critical national infrastructure systems, and those of our Allies, may be vulnerable to Cyber exploitation.

It's worth noting at this point that a strength of the UK system is that one organisation - GCHQ - brings together both disciplines. That arrangement is shared by only a few other countries, most notably the US . It gives us a richer view of vulnerabilities and threats than those who consider them purely from the point of view of defence.

So what do we know about the threat? This audience will be familiar with some of the Cyber incidents and concerns that have come up in the media. Without wishing to comment in detail on what we know about any specific stories, I will give you some general comment and context.

- It is true that we have seen worms cause significant disruption to Government systems – both those targeted deliberately against us, and those picked up from the Internet accidentally. There are over 20,000 malicious emails on Government networks each month, 1,000 of which are deliberately targeting them.
- It is true that we have seen the use of Cyber techniques by one nation on another to bring diplomatic or economic pressure to bear.
- It is true that we have seen theft of intellectual property on a massive scale, some of it not just

sensitive to the commercial enterprises in question but of national security concern too. As Jonathan Evans said in September, Cyberspace lowers the bar for entry to the espionage game, both for states and for criminal actors.

- And of course it is true that the risks in all these areas are growing along with the enormous growth of the Internet. At the moment it's expanding by about 60% a year. There are around ¼ of a trillion emails sent every day - even if 80% of these are spam. Cyberspace is contested every day, every hour, every minute, every second. I can vouch for that from the displays in our own operations centre of minute by minute cyber attempts to penetrate systems around the world.
- So Ministers are looking, in the context of the Strategic Defence and Security Review and the Spending Review, at what capabilities the UK needs

to develop further. Clearly they will also be deciding how they trade off against other spending priorities. I'll outline in a moment some of the things we might do, without prejudging any National Security Council decisions or SDSR announcement.

But first, one important message. Just because I, as a national security official, am giving a speech about Cyber, I don't want you to take away the impression that it is solely a national security or defence issue. It goes to the heart of our economic well-being and national interest.

Five perspectives

Let me illustrate that 'not just security' theme. I have five different perspectives on Cyber that I'd like to share with you today.

First, the Government wants to get **services on-line**. Most departments and Ministers aspire to put more and more Government activity on to the internet. It's a cheaper, faster, more efficient, way of running Government business. And it's a cheaper, faster, more efficient, and often more accessible way of delivering services directly to the public. The public increasingly *expects* services to be available online. But it has to be done without putting citizens' personal data at risk of being stolen, and without opening up payment systems to fraud. This is a big challenge. GCHQ's Information Assurance technical experts continue working — with the

Government Chief Information Officer and with the Office of Cyber Security in the Cabinet Office — to help Government departments address this challenge. Our professional rule of thumb is that good Information Assurance practice will solve 80% of Government's Cyber Security vulnerabilities. By this we mean observing basic network security disciplines like keeping patches up to date. That, combined with the necessary attention to personnel security and the 'insider' threat, will offer substantial protection for each individual network.

- But the scale of the challenge is changing; and the remaining 20% of the threat is complex and not easily addressed by just building the security walls higher and higher. As Bill Lynn, the US Deputy Secretary of Defense has said, a 'Maginot line' approach to defence will not be sufficient of itself. The 20% which is made up of that complex threat needs to be defended against in Cyberspace itself.

- Within the next few years on-line tax and benefit payment systems could be processing over one hundred billion pounds' worth of payments each year. There will be a public expectation that the citizen's transactions with Government will be protected. But criminal exploitation of those transactions need not be at the Government end. A Government network can be as well-protected in Information Assurance terms as you like but the stolen legitimate credentials of a citizen would still present a security problem. So those setting policies for public services, and those designing their delivery, need to be conscious of — and well-advised about — the wider Cyber Security aspects that might subvert their aims. And we need to deepen Government's dialogue and partnership with the Industry partners who deliver the systems and services that need securing. In many cases they

have an equal or greater stake in ensuring proper protection and realising efficiencies. There is a strong foundation on which to build in the structures that have been created under the Centre for the Protection of National Infrastructure and a number of Whitehall/industry bodies.

- Clear leadership at Ministerial level of Cyber Security and Information Assurance has been a great benefit in accelerating progress here.

My second theme. The **growth of e-crime** is disturbing. Accurate estimates for the overall costs to the economy are quite difficult to pin down but a figure well into the billions seems credible. At a more comprehensible level, hundreds of hacking forums exist. On them thousands of stolen UK credit card details are available for sale online for about 2 US dollars per set. Just one botnet is believed to have stolen credit card and online banking details from

up to 12.7million victims worldwide. This puts individual citizens at risk. And we have seen such botnets-for-hire used by organised criminal groups for concerted attempts to perpetrate multiple small frauds - not just against commercial targets but against online tax systems across Europe. e-Crime therefore begins to look like a low-risk, but potentially high-profit opportunity for the creative criminal. So we need to change that. The Law Enforcement and Intelligence communities are working to improve our collective approach to tackling it, developing the same kind of holistic approach that we use against the drugs trade. This would bring to bear a range of capabilities:

- strategic intelligence which tells us the overall scale and shape of the problem so we can focus interventions in the most effective place,
- Law Enforcement work to identify and tackle groups and individuals,

  - Pursuing offenders through the courts,
  - and measures to make it easier to identify and report criminal activity.

- As with other aspects of Cyber Security, we should seek to raise the cost to the adversary. Force criminals to work harder to achieve their aims and the problem should reduce. The owners of vulnerable services can help here by adhering to good Information Assurance practices.

A third theme. Much attention has been paid in the media to the potential for Cyber attacks to seriously disrupt **Critical National Infrastructure**. I would not wish to talk about the steps we take with the Security Service to reduce specific vulnerabilities. But the threat is a real and credible one. We already provide expert advice and incident response to the operators of critical services. We must continue to strengthen these capabilities and be

swifter in our response, aiming to match the speed at which cyber events happen. We need to consider the value of receiving in return a direct feed of information from the operators with that same sort of timeliness so that we are aware of the attacks that they are seeing on their systems as they happen. Of course that would need to be in proportion to the threat faced. But such feeds could give us the opportunity to respond, if necessary, with some active defensive techniques, as well as to spread knowledge of the threat quickly to others who may be vulnerable. For me this points to a different sort of partnership between the national security agencies and the key industry players. Our systems will need to be more interconnected. And we may need to establish different financial models to underpin a national capability which will be both public and private.

My next perspective. Cyber will involve us renewing our commitments to **international partnerships**. We have common interests with other nations in sharing information on threats and vulnerabilities. Again, this needs to happen at internet speed. Many of the enterprises or systems we are trying to protect extend across national boundaries. Even where a UK enterprise does not have some form of commercial partnership overseas, the communications systems on which it depends will almost certainly include servers and fibre optic cables in other countries. As our national abilities to defend our networks grow, the need for consensus amongst partners and allies on the right way to address specific threats will be ever more essential. We mustn't let differences between jurisdictions create a weak spot for attackers to exploit. Fortunately we have strong international alliances already that will help us to achieve this, in particular some of our intelligence and security

relationships. Through these relationships the UK is well placed to be a key player in international discussions and to play our part in an active and collective approach to defence.

- At the political and diplomatic level, we will need to reaffirm the proper norms of behaviour for responsible states in cyber space. Both how they should be expected to behave and what they should be able to expect from partners. When it comes to those who do not abide by the norms, one of the major difficulties we face is in attributing cyber activity to a particular nation state or other actor. It's not always impossible, but it is very, very hard. And that changes some of the military and diplomatic equations on how we deter, how we respond, how we counter or démarche. I think it would be fair to say we have not yet fully explored those strategic questions. For example, it may be possible to use

military Cyber capabilities for deterrent effect. But a casual parallel with nuclear deterrence and Mutually Assured Destruction is clearly wrong - because small scale but significant Cyber attacks happen every day. When it comes to these incidents, whether we can attribute the activity or not, we will need to have rapid and robust ways of working with allies. And where there is a deliberate or an unintended spread of a worm that threatens critical systems, counter-measures will need to be co-ordinated internationally in order to be effective.

Last but by no means least, and in fact fundamentally, getting Cyber right **enables the UK's continuing economic prosperity**. There's a clear defensive angle. In order to flourish, a knowledge economy needs to protect from exploitation the intellectual property at the heart of the creative and high-tech industry sectors. It needs to

maintain the integrity of its financial and commercial services. But I believe the prosperity implications of Cyber are wider than that. There is an opportunity which we can seize if Government and the telecommunications sector, hardware and software vendors, and managed service providers can come together. It's an opportunity to develop a holistic approach to Cyber Security that makes UK networks intrinsically resilient in the face of Cyber threats. And that will lead to a competitive advantage for the UK. We can give enterprises the confidence that by basing themselves here they gain the advantages of access to a modern internet infrastructure while reducing their risks. And developing such expertise also opens up potential export markets. The global market for cyber security products is growing faster than much of the rest of the global economy. We are seeing that potential market for UK products and services growing at over 10%

per annum. If we get the partnership approach right we can develop a thriving industry here.

Conclusion

In conclusion I'd like to leave you with some key themes that come out of what I've just said.

- Cyber is a real, live issue, bringing both threat and opportunity;
- It's not a narrow security issue for the spooks — but a wide economic issue that demands a holistic response.
- Perhaps 80% of what we need to do is stuff we already know how to do — getting the basics of Information Assurance right will of itself raise the bar for malicious activity.
- But 'patch and pray' will not be enough. At the national level, getting the rest of Cyber - the more difficult 20% - right will involve new technology, new partnerships, and investment in the right people. Crucial elements within that will be:

  - a different approach to Government-industry partnership,
  - and work by academia to broaden our research base and establish the mechanisms that will develop a large body of genuine expertise in the UK.

- But if we can get it right, then we have a real chance to keep our economy and our citizens secure. And, more than that, we can develop a world-class approach which potentially gives us a relative advantage — in security, military, and commercial spheres.

Thank you.