Speech

Chancellor's speech to GCHQ on cyber security

From:
HM Treasury, Government Communications Headquarters and The Rt Hon George Osborne MP
Delivered on:
17 November 2015 (Original script, may differ from delivered version)
Location:
GCHQ
First published:
17 November 2015
Part of:
Spending Review and Autumn Statement 2015

Chancellor lays out new plan for £1.9 billion cyber investment, and details seven more departments that have settled ahead of the Spending Review.

Before I start my speech, I want to say a few words about the heart-breaking events that unfolded in Paris on Friday evening.

This was an assault not just on the people of France, but on all of us who value freedom and democracy. We stand with the people of France. We know that we must act as one, just as our enemies see us as one.

As David Cameron has said, we will do everything we possibly can to help the French at this moment of national trauma. That includes making available to them the sharpest of our own national capability, which includes the skills and capabilities of GCHQ.

Before the dreadful events of the weekend we had already indicated that we would be increasing substantially the resources we dedicate to countering the terrorist threat posed by ISIL.

The Prime Minister has made clear that across the agencies a further 1,900 staff will be recruited to keep Britain safe from terrorist attack.

This was going to be an important outcome of the Spending Review. What has unfolded in Paris has reminded us all that it is a vital one too.

As the threat develops, we will need to make sure that our capabilities develop to match it. Following what happened to the Metrojet flight from Sharm, the Prime Minister announced that we would be doubling the amount we spent on aviation security.

The answer is not just in more resources, but in ensuring those who keep us safe have the right legal framework, that allows them to do their job while preserving the values and freedoms which we are so determined to defend.

Through the Investigatory Powers Bill, HM Government will make sure that they have the powers they need to access vital intelligence about the intentions and activities of those who wish us harm.

This determination to confront threats against our country is at the heart of what you do here at GCHQ.

To the men and women of GCHQ in this audience – the TV cameras today will not show your faces, and the public will never know your names, but let me say this: you are the unsung heroes who never get the recognition you deserve by dint of the sort of work you do, but who day and night keep us safe.

One of the ways you keep us safe is by tracking terrorist groups and collecting the information we need to stop those attacks.

Our intelligence agencies historically disrupt one terrorist plot a year; this year you have prevented seven. Let me thank you on behalf of the British people.

I also want to thank those of you in the audience who are here because you are our partners in keeping Britain safe in cyberspace – not just those from GCHQ, but across government, the armed forces, industry, and academia. For this is a shared effort between us.

Earlier this year the Prime Minister asked me to chair the government's committee on cyber, and through that I see the huge collective effort required to keep our country safe from cyber attack; the range of threats we face; and how this will be one of the great challenges of our lifetimes.

As Chancellor I know about the enormous potential for the internet to drive economic growth, but I am also acutely aware of the risk of cyber attack harming our economy and undermining the confidence on which it rests.

And I also know that we can’t afford to build strong cyber defences unless they rest on the solid foundations of sound public finances.

Next week I will present the conclusions of the Spending Review that will deliver those solid foundations. We have already reached provisional agreement with four departments, and today I can confirm we have provisionally settled a further seven Whitehall departments:

the Department for Energy and Climate Change

the Department for Work and Pensions

HM Revenue and Customs

the Cabinet Office

And the Scotland, Wales and Northern Ireland offices

This means that over half of the Whitehall departments have now reached provisional agreements on their resource budgets.

Combined, these departments will on average see a reduction in real terms spending of 24% by 2019-20, contributing to our economic security and enabling us to spend more on key priorities like national security. I’ve been very clear that we cannot afford national security without economic security.

But as we have seen in recent months and weeks, there will be no economic security for our country without national security.

Nowhere is that more true than when it comes to cyber.

When I was born the internet was barely two years old. It was the preserve of academics, used to connect dozens rather than billions of users. There weren’t many who predicted it would transform our world.

Today, the internet has changed our lives in countless ways, and continues to evolve at a pace that would have stunned even its own pioneers. Every part of the way we live is being touched and reshaped by it.

Britain helped create the internet – Tim Berners Lee created the World Wide Web, one of a long line of British scientists who have given us an outsized role in shaping our own digital future.

Britain is enriched by the internet. And Britain has embraced the internet – a far higher proportion of British retail is done online than in any other country in the world.

That’s an enormous economic and commercial opportunity for our country.

But when the internet was first created, it was built on trust.

That trust, appropriate inside a community of scholars, is not merited in a world with hostile powers, criminals and terrorists.

The internet has made us richer, freer, connected and informed in ways its founders could not have dreamt of. It has also become a vector of attack, espionage, crime and harm.

And that’s what I want to talk to you about this morning. For government has a duty to protect the country from cyber attack, and to ensure that the UK can defend itself in cyberspace.

Today I want to set out how we are fulfilling that duty. I will explain how we have invested in Britain’s cyber security in the past five years, and to set out our plan for the next five.

The national cyber plan I am announcing means investing in defending Britain in a cyber-age. It is a key part the Spending Review I will deliver next week.

For the Review is all about security: economic security, national security and the opportunity that comes to a country that provides that security.

It is right that we choose to invest in our cyber defences even at a time when we must cut other budgets.
For our country, defending our citizens from hostile powers, criminals or terrorists, the internet represents a critical axis of potential vulnerability.

From our banks to our cars, our military to our schools, whatever is online is also a target.

We see from this place every day the malign scope of our adversaries' goals, their warped sophistication and their frenetic activity.

The stakes could hardly be higher – if our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost.

ISIL's murderous brutality has a strong digital element.

At a time when so many others are using the internet to enhance freedom and give expression to liberal values and creativity, they are using it for evil.

Let's be clear

ISIL are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too.

They have not been able to use it to kill people yet by attacking our infrastructure through cyber attack They do not yet have that capability. But we know they want it, and are doing their best to build it.

So when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives.

It is one of the many cyber threats we are working to defeat.

Getting cyber security right requires new thinking. But certain principles remain true in cyberspace as they are true about security in the physical world.

Citizens need to follow basic rules of keeping themselves safe – installing security software, downloading software updates, using strong passwords.

Companies need to protect their own networks, and harden themselves against cyber attack.

The starting point must be that every British company is a target, that every British network will be attacked, and that cyber crime is not something that happens to other people

And government cannot duck its responsibilities. There are certain things that only government can do, in cyberspace just as in the physical world.

Government has a unique ability to aggregate and educate.

Only government can legislate and regulate. Only government can collect secret intelligence.

Government has a duty to protect the country from hostile attack. Government has a duty to protect its citizens and companies from crime.

Only government can defend against the most sophisticated threats, using its sovereign capability. And that's exactly what we will do.

And it is this sovereign capability that brings me here, to GCHQ.

Through my time in office, I have seen for myself the extraordinary quality of this institution; the dedication, integrity and ingenuity of its staff; and the difference it makes protecting our nation.

Coming here, as the first Chancellor to give a speech in GCHQ, I am acutely conscious of the rich history of this still relatively young institution in our island's story.

The father of GCHQ was Winston Churchill.

It was as First Lord of the Admiralty that he established Room 40, and gave it its charter. Room 40 was an operation to decrypt German communications during the First World War, a secret held on extraordinarily close hold even within government.

By 1924 Winston Churchill had become Chancellor of the Exchequer, and wrote to Prime Minister Stanley Baldwin saying:

In the years I have been in office since Room 40 began in the Autumn of 1914, I have read every one of its flimsies, and I attach more importance to them as a means of forming a true judgement of public policy in these spheres than to any other source of knowledge at the disposal of the state.

Churchill went on to complain that other ministers in the government had access to this information but that as Chancellor he did not, and that they therefore might have been pulling the wool over his eyes.

Some things have changed since those days. As a member of the National Security Council I see the crucial role that information produced by GCHQ can play in the conduct of government and war.

Other things haven't changed – like the continuing attempts by spending departments to pull the wool over the eyes of the Chancellor. A hundred years on, they still haven't learnt that it never, ever works.

GCHQ is rightly known as equal to the best in the world. And I am clear that the answer to the question 'who does cyber?' for the British government is – to very large degree – 'GCHQ'.

Of course there are others involved – the other intelligence agencies; the National Crime Agency; the Ministry of Defence; DCMS; the FCO.

Often in partnership with our Allies overseas, like the US and France. It's very good to see Matthew Barzun the American ambassador here this morning.

But GCHQ has a unique role. It is the point of deep expertise for the UK government. It has an unmatched understanding of the internet and of how to keep information safe.

It is a centre of capability that we cannot duplicate, which must sit at the heart of our cyber security.

Over the past 18 months, for example, GCHQ has helped UK law enforcement tackle a number of high-profile operations against pernicious cybercrime malware threats, like Dridex, Shylock and GameOver Zeus.

These have cost UK citizens and companies and government departments millions of pounds in the form of fraud, theft and damage; this figure would have been much higher had it not been for law enforcement disrupting these operations with GCHQ's help.

I can tell you today that right now GCHQ is monitoring cyber threats from high end adversaries against 450 companies across the aerospace, defence, energy, water, finance, transport and telecoms sectors.

In protecting the UK from cyber attack, we are not starting from zero.

In 2010, at a time when we as a new government were taking the most difficult decisions on spending in other areas, we took a deliberate decision to increase spending on cyber.

We set up the National Cyber Security Programme and funded it with £860 million.

And for the past five years we have been creating and enhancing the structures and capabilities that Britain needs to defend itself in cyberspace.

We have invested in building our sovereign capability here at GCHQ.

We have ensured that our military systems are properly secured from cyber attack.

We have built the National Cyber Crime Unit so cyber criminals are brought to justice.

We established the Computer Emergency Response Team for the UK, and the Cyber Information Sharing Partnership so companies could share what they knew.

We developed clear guidance for businesses, including the Cyber Essentials scheme, which already has over a thousand companies accredited.

We launched a series of cyber risk reviews for companies in the Critical National Infrastructure, to identify vulnerabilities that could then be addressed.

We built cyber security into every stage of the education process. We established Cyber First and cyber apprentices to make sure that we got the talent we needed coming into the field.

And we undertake exercises so we know what to do when there is a serious cyber incident.

One such exercise took place last week – Resilient Shield, a joint UK/US exercise across the financial sector.

So I want to thank all those who, over the last five years, have brought us to where we are today.

We have built a world-class range of tools and capabilities that Britain needs to stay safe from cyber attack.

We are widely regarded as top or near top in the world.

But nice though it would be to sit on our laurels, the truth is that we are not where we need to be. We are not winning as often as we need to against those who would hurt us in cyberspace.

The truth is that we have to run simply to stand still.

The pace of innovation of cyber attack is breathtakingly fast, and defending Britain means that we have to keep up.

At the heart of cyber security is a painful asymmetry between attack and defence.

It is easier and cheaper to attack a network than it is to defend it. And the truth is that this asymmetry is growing.

A few years ago mounting a sophisticated cyber attack meant having all the skills that each stage of the attack required, from gaining access to the network to designing the payload that was to go into it.

But in the past few years, an on-line market-place has developed, which means all the elements of an attack can now be bought and assembled from the computer of anyone with the money to pay for it.

The barriers to entry are coming right down, and so the task of the defenders is becoming harder.

All of this is reflected in the cyber breaches that we see reported with increasing frequency and increasing severity.

Last summer GCHQ dealt with 100 cyber national security incidents per month. This summer, the figure was 200 a month. Each of these attacks damages companies, their customers, and the public's trust in our collective ability to keep their data and privacy safe.

Imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the internet that we need for our online economy and social life to function.

As a nation determined to live within our means, we are facing painful choices, and the hardest of decisions. You will see that next week.

But the Prime Minister, my colleagues at the top of government and I have decided that we have to make a top priority of cyber security, if Britain is to be able to defend itself, now and in the future.

Today I am announcing a plan to do precisely that.

It is a bold, comprehensive programme that will give Britain the next generation of cyber security, and make Britain one of the safest places to do business online.

It will give our companies and our citizens confidence that their cyber-safety is being properly protected. It will ensure that Britain remains at the cutting edge of the global cyber economy.

In the Spending Review, I have made a provision to almost double our investment to protect Britain from cyber attack and develop our sovereign capabilities in cyberspace, totalling £1.9 billion over five years.

If you add together the spending on core cyber security capabilities, protecting our own networks and ensuring safe and secure online services, the government's total cyber spending will be more than £3.2 billion.

That money by itself is not enough. It supports a national cyber plan.

The plan consists of five major steps forward in the nation's cyber defence.

The most fundamental thing we need to do is defend ourselves online, and we are developing a series of measures to do so more actively.

We will be stepping up our efforts to disrupt the criminal marketplace, and making sure that anyone committing cyber crime against our citizens and companies will be brought to justice.

We will be boosting the capabilities of the National Cyber Crime Unit, so that – in partnership with their counterparts around the world - they attack the assumption among too many that cyber crime is risk free, and comes with little risk of consequences.

We will introduce stronger defences for government systems.

We will aggressively defend our public services from cyber attack by installing capabilities that can detect attacks, find where our services are vulnerable to attack, and fix them.

We will introduce a cross-government IP Reputation Service – warning government websites when they try to do business with known bad addresses.

We have done this already with HMRC, and saved £40 million on fraud on a £1 million investment.

But we can go further.

Internet service providers already divert their customers from known bad addresses, to prevent them from being infected with malware.

We will explore whether they can work together – with our help – to provide this protection on a national level.

We cannot create a hermetic seal around the country – indeed it wouldn’t be in our interests to have one – but with the right systems and tools our private internet service providers could kick out a high proportion of the malware in the UK internet, and block the addresses which we know are doing nothing but scamming, tricking and attacking British internet users.

Let us try to get to the point where all the internet service providers will as a matter of routine divert known bad addresses.

By doing so, we could fundamentally alter the economics of cyber crime against UK citizens and businesses.

Second, we need to address the alphabet soup of agencies involved in protecting Britain in cyberspace.

As the threat has emerged, so have they. Now we need to bring more coherence to our efforts, so that businesses know there is a single place they can go for advice and help.

Today I can announce that in 2016 we will establish a single National Cyber Centre, which will report to the Director of GCHQ.

The Centre will be a unified source of advice and support for the economy, replacing the current array of bodies with a single point of contact.

The Centre will make it easier for industry to get the support it needs from government. And make it easier for government and industry to share information on the cyber threat to protect the UK.

Reporting to GCHQ will mean the Centre can draw on the necessarily secret world-class expertise within this organisation.

But the Centre will also have a strong public face and will work hand in hand with industry, academia and international partners to keep the UK protected against cyber attacks.

And over time, we will build several important capabilities in the new Centre. It will give us a unified platform to handle incidents as they arise, ensuring a faster and more effective response to major attacks.

And we will build in the National Cyber Centre a series of teams, expert in the cyber security of their own sectors, from banking to aviation, but able to draw on the deep expertise here, and advise companies, regulators, and government departments.

Building the National Cyber Centre will be a hugely ambitious and important undertaking that reflects this government's commitment to making the UK secure in cyberspace.

The third part of the plan is about the most important raw material.

We will never succeed in keeping Britain safe in cyberspace unless we have more people with the cyber skills that we need. This year's Global Information Security Workforce Study estimates that the global cyber security workforce shortage will widen to 1.5 million by 2020.

If we do not act decisively, the skills gap will grow, and limit everything we want to achieve in cyberspace.
So we will launch an ambitious programme to build the cyber skills our country needs, identifying young people with cyber talent, training them, and giving them a diversity of routes into cyber careers.

Training the next generation of coders is vital – both for our economy and our security.

Today I can announce that, as part of the Spending Review we will be running a £20 million competition to open a new Institute of Coding to fill the current gap in higher education and train the next generation in the high level digital and computer science skills that we need.

We will invite bids – including joint bids – from our universities, businesses and others who have the innovative ideas to bring these proposals to life.

As all of you who work in the sector know, what is needed are specific cyber security skills, building on particular talents.

And we need to tackle this problem on a number of fronts including in our universities. But we need to make sure there are other routes into the cyber workforce.

So we will build higher and degree level apprenticeships in key sectors, starting with the finance and energy sectors. We will create a retraining programme for highly skilled workers who want to move into cyber.

And most ambitiously, we will be rolling out a major programme for the most talented 14 to 17 year olds, involving after-school sessions with expert mentors, challenging projects, and summer schools where those on the scheme can see where their cyber skills can take them.

Modelled on a hugely successful Israeli programme, this scheme will help us draw on the great hidden talents in our classrooms and bring on our nation’s cyber potential.

Of course, we need not just great skills but great British companies as well.

If Britain is to be a world leader in cyber, and stay at the cutting edge of cyber technology, we need the innovation and vigour that only these companies can offer.

We need to create a commercial ecosystem in which cyber start-ups proliferate, get the investment and support they need, and are helped to win business around the world.

We need an ecosystem in which our best people move in and out of institutions like this one, bringing the best minds and deepest expertise into the private sector, and the latest innovation back into government.

We need an ecosystem in which great ideas get translated into great companies.

So the fourth element of the plan is to set up programmes to support the best cyber start-ups – excellent British companies like GlassWall, Garrison, Digital Shadows and Titania, who I am glad to see here with us.

I am glad that there is already so much happening in this space; I am happy we have the founders of Cyber London with us today.

And I am delighted that Paladin Capital has just announced it is establishing a dedicated cyber fund in the UK; we can be proud that they have chosen London as its base.

We will build on this energy. We will help commercialise the extraordinary innovation in our universities. We will provide training and mentoring for our cyber entrepreneurs.

We will be establishing two cyber innovation centres - places where cyber start-ups can base themselves in their crucial early months, and which can become platforms for giving those start-ups the best possible support.

I have talked before about an arc of cyber excellence – stretching from this building, through Bristol and Bath to Exeter – to make the South West a world leader in Cyber Security.

Today I can announce that one of the two innovation centres will be here in the South West of England, in Cheltenham, reflecting the extraordinary talent in this place, and our aspiration that this talent should help drive our cyber sector.

Government can itself provide a huge boost for British cyber start-ups, if it can be smart enough to marshal its procurement in a coherent way.

This should be a win-win – our cyber start-ups need endorsement, investment and first customers.

And government, from our military and GCHQ to the Government Digital Service and the NHS, need to be able to procure excellent cyber security hardware and services.

So I can announce today that we will create a £165 million Defence and Cyber Innovation Fund, to support innovative procurement across both defence and cyber security.

It will mean that we support our cyber sector at the same time as investing in solutions to the hardest cyber problems that government faces.

Of course, our involvement with industry on cyber goes well beyond the cyber sector. We need to make sure that Britain has the regulatory framework it needs, particularly in the sectors we define as the Critical National Infrastructure.

If the lights go out, the banks stop working, the hospitals stop functioning or government itself can no longer operate, the impact on society could be catastrophic.

So government has a responsibility towards these sectors, and the companies in those sectors have a responsibility to ensure their own resilience.

Any new regulation will need to be carefully done – light enough and supple enough that it can keep up with the threat, so it encourages growth and innovation rather than suffocates it.

Our vulnerability as a nation in cyberspace goes well beyond the critical national infrastructure.

The impact of last year's attack on Sony should be a warning to anyone who thinks that such attacks are just a matter for the companies concerned.

We have a collective interest in the cyber defences of individual companies across the British economy.

The experience in the last month of TalkTalk shows how cyber attack can suddenly go from a theoretical risk to a massive business cost.

We will work with businesses across the economy to ensure that they have the right defences in place.

All of this sets out what we will do to establish the strongest possible defences for Britain.

Strong defences are necessary for our long-term security. But the capacity to attack is also a form of defence.

If we are to tackle the asymmetry between attack and defence, then we need to establish deterrence in cyberspace.

We need not just to defend ourselves against attacks, but rather to dissuade people and states from targeting us in the first place.

Part of establishing deterrence will be making ourselves a difficult target, so that doing us damage in cyberspace is neither cheap nor easy.

Part of establishing deterrence will be building global norms, so that those who do not follow them can be called out, and shown to be acting outside the boundaries of acceptable behaviour.

And part of establishing deterrence will be making sure that whoever attacks us knows we are able to hit back.
We need to destroy the idea that there is impunity in cyberspace.

We need those who would harm us to know that we will defend ourselves robustly. And that we have the means to do so.

This is the fifth element of the plan.

Thanks to the investment that we have made during the last Parliament, just as our adversaries can use a range of actions against us, from the virtual to the physical, so we are making sure that we can employ a full spectrum of actions in response.

We reserve the right to respond to a cyber attack in any way that we choose.

And we are ensuring that we have at our disposal the tools and capabilities we need to respond as we need to protect this nation, in cyberspace just as in the physical realm.

We are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace.
We have built this capability through investing in a National Offensive Cyber Programme.

The Programme is a partnership between the Ministry of Defence and GCHQ, harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required for the UK to establish a world class capability.

And we will now commit the resources to develop and improve this capability over the next five years.

The threats to our country in cyber space come from a range of places – from individual hackers, criminal gangs, terrorist groups and hostile powers.

To all of them I have a clear message.

We will defend ourselves. But we will also take the fight to you too.

We are increasingly confident in our ability to determine from where attacks come.

We are stepping up not just the means of defence, but also the means to ensure that attacks on Britain are not cost-free.

To those who believe that cyber attack can be done with impunity I say this: that impunity no longer exists.

And at the sharpest end, we need to ensure that our military are equipped to fight the wars of the 21st Century.

That means they need to be prepared for hybrid conflicts, played out in cyberspace as well as on the battlefield. A 21st Century military has to operate as effectively in cyberspace as it does on land and sea, in the air and space.

Our commitment to spending 2% GDP on defence means we can invest in a military that is cyber trained, cyber secure, and cyber enabled, with the ability to fight in every domain of future conflicts.

The PM will set out more details in the Security and Defence Strategic Review.

Of course the internet is global, and so must our approach be.

We need to keep fighting to preserve a free, open, peaceful and secure cyberspace.

Agreement that international law applies in cyberspace has been an essential first step.

And we need international norms of behaviour in cyberspace, so that freedom is matched by responsibility.

Norms like working together to prosecute those who commit illegal acts online; like not deliberately allowing their territory to be used for internationally wrongful acts; like not illegally preventing critical infrastructure from delivering essential services to the public.

We do all this by creating the strongest possible alliance of like-minded states that share our vision.

We will do this by showing to those that have a different view of the internet that our approach can bring all of us benefits – just as we have done by encouraging Huawei to invest safely in the UK though partnership with GCHQ.

We need our police forces to work together to ensure that less and less of the world is a hiding place for cyber criminals.

And we need to help our partners develop their own cyber-security – as we share a single cyberspace, we collectively become stronger when each country improves its own defences.

For the past five years we have been investing in the cyber security of our partners as well as our own.

We have helped establish the outstanding Global Cyber Security Capacity Centre in Oxford. In the coming years we will step up these efforts, mindful that we are bound together in cyberspace.

The national cyber plan that I have announced today is bold, far-reaching and transformative in numerous ways.

It will provide the next generation of cyber security for our country.

It will ensure that we have the skills, the structures, the tools, the companies and the partners we need.
It will not be enough to stop Britain being attacked every minute of every day. It will not prevent breaches, or provide hermetic protection for the country or any part of it.

But it will make Britain one of the best protected countries in the world; it will give our companies and citizens the tools they need to stay safe from cyber attack; and it will create jobs and prosperity.

With the ability and dedication of GCHQ’s staff, our new National Cyber Centre, and the ideas and skills across our country, our plan will make sure that Britain remains a world leader in cyber, and give Britain an important edge in the global race.

And just as we build our resilience to cyber attack, so too we will keep building our resilience to terrorist attacks – in all their evil and murderous forms.

This requires effort by all of us – government and industry, start-ups and universities, agencies and allies.

You are each here because we need you to be our partners in this great task.

And – hard though this task will be – I know that we will succeed.