

Speech: MI6 'C' speech on fourth generation espionage

Ladies and Gentlemen, it is a pleasure to be back at St Andrews. I had no idea that I would return one day as Chief of the Secret Intelligence Service, SIS – as we call ourselves – or MI6, as we are known to the world. After I graduated, I joined a Scottish Regiment. But within 4 years I found myself sitting in MI6 Headquarters, staring at a blank piece of paper. I imagine some of you might be familiar with that situation.

I had been given, as my first job, the task of penetrating an organisation intent on genocide in the Western Balkans in the mid-1990s.

Starting from that blank piece of paper, I had to find my way to the heart of that organisation and obtain secret information for the British government.

It took me to places I never thought I would visit, often travelling under a false identity. It involved many nights drinking obscure homemade alcohol, piecing together the intentions of the parties to that conflict, and allowing me to create the secret relationships necessary to provide the intelligence our country urgently needed.

I had the satisfaction of knowing that my work, along with that of many others, helped to pave the way for the eventual arrest and prosecution of war criminals implicated in the murder or displacement of hundreds of thousands of people.

Intelligence work on its own can't stop every attack or prevent every evil. But it can shorten wars, and it can and does save lives.

That sense of pride at being part of an effort and cause greater than myself has never left me for a single day of nearly 30 years serving my country as an intelligence officer. I believe this to be true of every member of our organisation.

When I look back on those early days of my work with MI6 and ask myself how I was able to do it, I realise that it owes a great deal to this university. More than I knew at the time, St Andrews shaped me as a person.

The – how shall I put it – lack of distraction in this corner of Fife lends itself to deeper human relationships than are typical of university life.

St Andrews taught me to think in an open-minded way about the world. It taught me the value of the human curiosity and curiosity about humans that has propelled my career, and the career of the surprisingly large number of St Andrews graduates in the ranks of SIS.

For if you strip away the mystique that envelops our organisation, that is our fundamental role: we provide human intelligence.

Our task is to create human relationships that bridge forbidding cultural and linguistic boundaries, in some of the most challenging environments on earth and online. We do this for a specific reason: in order to obtain information and take actions required by the British government to keep this country safe.

Our skill lies in our ability to create relationships of trust between our officers and people inside the organisations we need to understand. We call these brave people agents, and they put their livelihoods, and sometimes even their lives, at risk on behalf of the United Kingdom. That is why our people, our methods and our operations must always remain secret.

While I'm going to speak today about how the world is changing and SIS is changing with it, I do not expect our human intelligence role will ever change fundamentally. We will always need to understand the motivations, intentions and aspirations of people in other countries. Even in an era of artificial intelligence you need human intelligence, in fact it will become even more important in a more complex world.

The degree of interconnectedness between nations, peoples and systems today, the ubiquitous nature of information, and the exponential pace of technological change, are making the world dramatically more complicated.

This complexity has eroded the boundaries we have traditionally relied upon for our security: the boundaries between virtual and real, the domestic and the international, between states and non-state actors and between war and peace. The result is a world of far greater ambiguity.

I want to be clear: our adversaries did not create this ambiguity and they did not create the things that divide us.

But they have shown a keen willingness to exploit ambiguity in an opportunistic way, taking advantage of blurred lines to probe our institutions and defences in ways that fall short of traditional warfare.

We refer to these as hybrid threats. They include the cyber attacks, misinformation and disguised use of military force seen in Ukraine and elsewhere, combined with political obfuscation, or what you might call implausible deniability.

The good news is that we are far from powerless when confronted by these challenges.

We are better placed than most countries to cope with a world of hybrid threats, because of the strength of our alliances, our values, and our institutions. This includes the UK intelligence community. After all, ambiguity is the state SIS is constituted to dispel, but it is also the context in which we operate. We are at home with ambiguity. It is a new environment, but it is our traditional business.

We are one of the few truly global intelligence agencies, capable of going to the source of problems anywhere in the world to recruit and run secret agents, penetrate terrorist organisations, provide our government with the

intelligence it needs to safeguard the national interest, give UK authorities information they need to disrupt terrorist attacks at home and against our allies, and detect and counter efforts by state and non-state actors to traffic drugs or proliferate nuclear and chemical weapons.

So SIS's mission is a crucial aspect of our strength as a democracy, and as a member of the Western Alliance in the 21st century.

As Chief I rarely speak in public. I am a spy. And less is more. This is only my second public speech in 4 years; and you might have to wait quite a long time for another one.

But I am speaking today because it is vital that people hear enough about SIS to know what we really do – as opposed to the myths about what we do – and because we want talented young people across our country to join us.

While I am delighted to say that we recruit the very brightest talent, and have extraordinary young people working in our organisation, this is not something I will ever take for granted. We are going to need the most diverse and skilled officers possible in the years ahead. Because the reality of the world is going to become more ambiguous, and more complicated.

While I was St Andrews I also studied computer science. The radical thought in those days was that computers would soon be able to talk to each other. Now, billions of people and devices are connected worldwide.

We are in the early stages of a fourth industrial revolution that will further blur the lines between the physical, the digital and biological realms. Lawfully used, technology such as bulk data, modern analytics and machine learning is a golden opportunity for society at large, including for MI6 as an organisation.

But I have also witnessed the damage new technologies can do in the hands of a skilled opponent unrestrained by any notion of law or morality, as well as the potentially existential challenge the data age poses to the traditional operating methods of a secret intelligence agency. We and our allies face a battle to make sure technology works to our advantage, not to that of our opponents. Liberal democracies should approach this with confidence, as the originators of this technology.

But the twin drivers of technological change and international complexity mean that we have to keep adapting if we are to be as effective at spying in the future as we are today. There will be a dividing line between those Intelligence Services that grasp this, as the UK agencies have, and those services that don't.

The era of the fourth industrial revolution calls for a fourth generation espionage: fusing our traditional human skills with accelerated innovation, new partnerships and a mindset that mobilises diversity and empowers the young.

Across the century of SIS's existence, we have evolved continuously to confront each generation of threat: from the World Wars to the Cold War to

the rise of transnational threats including international terrorism. Now, we are evolving again to meet the threats of the hybrid age – the fourth generation I am speaking of.

This evolution takes 3 forms, that I want to describe to you:

First, when your defences as a country are being probed on multiple fronts at the same time, it can be difficult to see the totality of what your opponent is trying to do. Security in the hybrid world is therefore all about who can partner to the greatest effect.

In the UK, we call this the Fusion Doctrine, and it involves drawing together all our national capabilities to detect, deter and counter hybrid attacks and other threats to the United Kingdom.

When I joined SIS, operations were largely conducted by individuals, as the story of my blank sheet of paper on my first mission suggests.

We now operate dynamic teams that draw on skills and knowledge across the whole of SIS: bringing together the formidable talents of our agent recruiters and runners, our analysts, our subject matter experts, our linguists, our data scientists and our technical and engineering officers – known to the public as Q branch.

We work more closely than ever before with our sister agencies M15 and GCHQ. We each have a distinct mission and culture, but we have found that everything we do is interdependent, and we have made a virtue of this. We are among the most closely integrated intelligence communities in the world.

The spirit of partnership extends further, to the police and other domestic agencies, the Foreign and Commonwealth Office and the Ministry of Defence, and the UK Armed Forces we often serve alongside.

We also draw on unparalleled partnerships overseas, including our Five Eyes allies the United States, Canada, New Zealand and Australia, and our close and historic security relationships across Europe.

The implications of the Brexit debate have been set out by Ministers. For our part as SIS, we will always work with our sister agencies to strengthen our indispensable security ties in Europe.

We also work with other partners across the world, to disrupt terrorist activity and counter other serious threats – but always on our terms, and based on our laws and our values as the United Kingdom.

When you consider these concentric circles of partnership, and the breadth of skill, experience and trust that they encompass, it is not surprising that adversaries seek to offset their relative disadvantage through hybrid means. Indeed, when they can they will take steps to undermine these partnerships, and we must take action of our own kind in response.

So second, alongside our core mission of revealing the intentions of adversaries and giving the UK government strategic advantage overseas, our

task now is to master covert action in the data age.

When I joined SIS, our principal task was finding out secrets. In a world of hybrid threats it is not enough to know what your adversary is doing. You must be able to take steps to change their behaviour.

This is primarily driven by the threat from terrorism – the ultimate manifestation of the eroded boundaries of the 21st century. SIS is the arm of government that has the ability to go overseas to the source of terrorist threats, and to disrupt them lawfully through our partnerships.

And I can tell you today, that since my last speech, we and our sister agencies have disrupted multiple serious Daesh attack plans originating overseas that, if successful, would have caused significant loss of life.

This includes an important contribution to helping European countries, particularly our French and German allies, prevent terrorist attacks in their countries or against their citizens.

This has involved exceptionally difficult and dangerous work. We have asked our agents – the people who agree to work in secret for MI6 – to do extraordinary things and run great risks. And I will not hide from you that some have paid the ultimate price. Our country and our allies owe them a debt they can never truly know and never fully repay.

We are proud of the contribution we have made to the coalition action in Syria which has now come close to destroying the so-called Caliphate. This has had a welcome effect on the direct threat to Europe. But to be clear, if the tragic events of 2017 in the UK are not sufficient of a reminder, we face a persistent and evolving threat from terrorism, one that demands that we evolve in turn.

You might think that countering terrorism was challenging enough. But now we face the additional complexity of the threats posed by nation states operating in the grey spaces of the hybrid era, which is a wholly separate problem.

Article 5 of the North Atlantic Treaty, which states that an armed attack against one or more of the NATO allies will be considered an attack on all, is the cornerstone of our defence and security. But it presupposes a clear distinction between a condition of war and a condition of peace – precisely the distinction that our opponents are seeking to obscure.

As allies we are determined to uphold and deepen our Article 5 commitment to each other's security. But it is significant that we face adversaries who now regard themselves as being in a state of perpetual confrontation with us.

One of the most egregious examples of this was the attack in Salisbury, in which the Russian state used a military-grade chemical weapon on UK soil.

We did not respond to this flagrant hostile act by emulating Russian tactics. Instead, we operationalised our values, our legal system, and our alliances. We exposed the perpetrators and coordinated the [largest ever collective](#)

[expulsion of Russian intelligence officers](#) from NATO and partner states, significantly degrading Russian intelligence capability.

When faced by these kinds of attacks, our approach with our allies is to seek to attach a cost to the behaviour. Our intention is for the Russian state to conclude that, whatever benefits it thinks it is accruing from this activity, they are not worth the risk.

We will do this in our way, according to our laws, and our values. We will be successful nonetheless, and I urge Russia or any other state intent on subverting our way of life not to underestimate our determination and our capabilities, or those of our allies. We can do this to any opponent at any time.

But I should emphasise that even as the Russian state seeks to destabilise us, we do not seek to destabilise Russia. We do not seek an escalation. If we see a change in Russian behaviour, we will respond positively. But we will be implacable in defence of our people and our vital interests.

We will continue to defend the rule of law and the international rules-based system robustly.

Our allies trusted in our intelligence in the aftermath of the Salisbury attack. We felt this as an act of solidarity and it meant a huge amount to us. But we have been clear to our allies that it was an act of self-interest on their part as much as one of solidarity. Whatever an adversary can do to us they can and have done to others.

Our approach to attaching a cost to malign activity also applies to cyber attacks, as in March this year when the [UK attributed responsibility for the NotPetya attack](#) against Ukraine, which also affected the United Kingdom, to the Russian government.

Much of the evolving state threat is about our opponents' increasingly innovative exploitation of modern technology. So simply put, we've got to innovate faster than they can. Indeed, future generations would not forgive us if it were otherwise.

This brings me to the third driver for change in SIS: the need to ensure that technology is on our side, not that of our opponents.

The digital era has profoundly changed our operating environment. Bulk data combined with modern analytics make the modern world transparent, a fact which contributed to GRU embarrassment after the Salisbury attack. But it is also a serious challenge if used against us.

So we are evolving rapidly. Cyber is now our fastest-growing directorate. We are shifting our focus to the nexus between humans and technology. And for the first time, through the National Security Strategic Investment Fund, we are pursuing a completely different type of partnership with the tech-innovation community, giving the private and academic community the role we need and they deserve.

Ironically, the most profound consequence of the technological challenge is a human one. We are determined, of course, to attract people with an even higher level of technical skill to join our ranks, in the best traditions of Q. But my organisation will need to adapt even faster if it is to thrive in the future. And that will require people with new perspectives, capable of harnessing their creativity in ways that we can't yet even imagine.

It is why we are determined to attract people from the widest range of backgrounds to join SIS. This will enable us to bring the widest range of approaches to bear on solving complex problems and so make our missions even more effective.

People sometimes ask what causes me to lose most sleep at night. The answer might surprise you. The biggest risk that I see is a failure to make full use of the amazing talent in our organisation and in our country at large. As the leadership of MI6 we are determined not to let that happen.

I believe in empowering those closest to the problem with the skills and authority they need to solve it. We delegate assertively. In the cyber age, newcomers will often be better equipped to solve problems than those, like me, steeped in experience can be. If you join us, you will be trusted to use your talents.

I have spoken of how SIS is pioneering a fourth generation of espionage – deepening our partnerships to counter hybrid threats, mastering covert action in the data age, attaching a cost to malign activity by adversaries and innovating to ensure that technology works to our advantage.

But while all these things change, there is one thing that will not alter, and about which there is no ambiguity, and that is our commitment to the values and laws of the United Kingdom.

We understand that what we do we do in the public's name, and that public confidence in what we do is fundamental to our success. Above all, we know that if we undermined our values even in the process of defending them, then we would have failed.

SIS operates in secret, but secret does not mean unaccountable. Our actions are tasked and authorised by ministers and carried out only in support of government policies. And we are answerable to independent scrutiny by the Investigatory Powers Commissioners and oversight by Parliament's Intelligence and Security Committee.

Alongside this duty to be accountable we of course have a duty to learn the lessons of the past.

I am one of the many SIS officers who have served in Afghanistan. After the 9/11 attacks I witnessed at every level in SIS a profound impulse to step forward into the line of danger. We felt that our organisation was one of the few that could make a difference, faced with a wholly new, and open-ended, threat from international terrorism.

I am proud of the courage and reflex to do the right thing that SIS

demonstrated. But the government has acknowledged in its response to the Intelligence and Security Committee's recent report, that we were not fully prepared for the challenges that we faced in those fraught times. Some of our officers were sent into a situation for which they were not fully prepared, and it took SIS too long to rectify that.

The report made hard reading for those of us who want our service to be the best it can be. But be in no doubt that we will learn the lessons.

So fifteen years later, we have improved our operational policy and practice, strengthened our training and guidance, and we now operate within an enhanced oversight and operational framework. And I'm proud that the Committee also concluded that SIS has the values and resilience to meet the current counter-terrorism challenge.

Above all, I have unshakeable faith in the quality, humanity and decency of the men and women who choose to join SIS. When faced with some of the very worst behaviour and dangers that humanity can devise, their instinct is to put themselves forward in the service of their country, and their fellow men and women.

We want people from across our country who feel a similar call to service to [consider applying to join our ranks](#).

I have spoken at St Andrews today because of the deep affection I have for this university, and because you are one of the best in the world for the study of terrorism, international relations and artificial intelligence. But my message is to students in every school, college and university across our country. In particular, I want to speak to young people who have never seen themselves in MI6.

The stereotype is that we only want a certain "type" to join MI6. This is false. If you think you can spot an MI6 officer, you are mistaken. It doesn't matter where you are from. If you want to make a difference and you think you might have what it takes, then the chances are that you do have what it takes, and we hope you will step forward.

It is the greatest honour of my career to lead the women and men of MI6. I believe the more you knew about what they were doing the prouder you would be.

You can tell a lot about the soul of a country from its intelligence services. In SIS, we have a service rooted in and inspired by the values of liberal democracy, determined to defend our country and the international rule of law, and carrying out remarkable and highly effective work in the face of potent threats, with creativity and courage and integrity.

These are the qualities that allow us to be the secret front line, to stand between this country and danger, and to help create an international environment in which our country and our people can prosper and thrive.

Thank you very much.