WADHAM LECTURE – 8th May, 2014, Wadham College, Oxford

"Intelligence Agencies in the Internet Age - Public Servants or Public Threat?"

Sir Malcolm Rifkind MP
Chairman of the Intelligence and Security Committee of Parliament.

I am very pleased to be able to give this Lecture at Wadham College. I am strongly of the view that more public debate about intelligence and the role of our Intelligence Agencies is vital in Britain.

I begin by observing that Intelligence Agencies in any free society should not be treated with unqualified enthusiasm.

Firstly, they are secretive, and must remain so as regards a very high proportion of their capabilities and activities. This, inevitably, makes it much more difficult for Parliament, the press and civil society as a whole in holding them to account than with any other part of Government or of the public sector.

Furthermore, to fulfil their statutory responsibilities and serve the public interest they must be given lawful authority to carry out deeds which, if carried out by any other citizen, would constitute criminal offences . They have legal authority to hack computers, intercept phones or break into peoples homes to plant bugs. In any democracy that should make all of us uncomfortable.

For the public to accept such powers there needs to be proper oversight of the agencies. But, it is unavoidable that that oversight can only be exercised by people permitted to have access to the secret information that the Agencies gather. Apart from senior Ministers and a small handful of public servants, that access is limited to the quasi-judicial Commissioners and to the Intelligence and Security Committee of Parliament, which I chair.

If the public are to be supportive of the work of the Intelligence Agencies they must not only have trust in them but also in the independence and integrity of those who carry out the oversight task.

Some of the secrecy which used to surround the Agencies has gone. Today, the intelligence chiefs are questioned in front of the TV cameras; their names are known as are their places of work, in Vauxhall, Thames House and Cheltenham, to a degree that would have been inconceivable even thirty years ago. But although there has been much greater openness there needs, also, to be continuing examination as to whether transparency can be further enhanced and secrecy modified without harm to their operational effectiveness.

During these years of increasing openness, the priorities of the Agencies and the technical capabilities available, not only to them but also to those who would do us harm, have changed out of all recognition. The advent of the internet age and its implications for the world of intelligence is, perhaps, the profoundest change of all.

For many years the primary purpose of our secret services was to find out the secrets of hostile governments and their leaders; to protect the secrets of our own government, and guard against internal subversion. Espionage and counter-espionage were the classic priorities.

Activity of this kind is as old as the hills. Parliament first established an account to properly fund the collection of secret intelligence in 1689. In 1807, when Napoleon and Tsar Alexander I were sat on Napoleon's barge at Tilsit negotiating a joint invasion of British India, a Russian aristocrat recruited by the British secret service and stationed in the water underneath the barge listened in on their conversation and reported it to London.

In the twentieth century intelligence capabilities and those of our adversaries were revolutionised by developments in signals intelligence technology. In 1917, British intelligence famously intercepted a telegram communicated via undersea cables from the German Foreign Minister, Arthur Zimmermann, to Mexico - enjoining the Mexicans to join the Central Powers in exchange, after German victory, for the recovery of their lost territory in Texas, New Mexico, and Arizona. The Mexicans, very wisely, were not impressed.

During the Cold War, despite continuing developments in technology, spying was still largely conducted at a state-to-state level. The IRA campaign in Northern Ireland and on the British mainland was the one significant exception.

After the Soviet Union collapsed, the spies were brought in from the cold. The resources and manpower of the Agencies were substantially scaled down.

Then, the tragic events of 11th September 2001 in New York, and the London bombings in 2005 changed everything. They brought home the realisation that rather than hostile governments, international terrorist organisations now posed the most serious threat to the safety of the public. Furthermore, as we found in 2005, many of these terrorists had not come from abroad but were British citizens so alienated from our society and values that they were prepared not only to blow themselves up but to take with them as many of their fellow citizens as they could.

Over the last decade or so Western intelligence agencies have therefore had to make international counter-terrorism, rather than espionage or counter-espionage, their major concern.

At the heart of the development of the international terror networks that most threaten our safety is the rise and spread of the internet. Global terrorists communicate globally, and in practice this means communicating online, using e-mail, social messaging, peer-to-peer sharing sites, chat rooms, webcams, online gaming platforms, mobile applications and a whole host of other media. It allows extremists to disseminate propaganda, attract and radicalise sympathisers, and ultimately to organise and prepare acts of terror, without ever having to meet face-to-face.

Just as many millions of Britons use the Internet to stay in touch with people in the UK and abroad; so many young Britons, already radicalised or at risk of radicalisation, are in regular contact with people in remote, distant, hostile or ungoverned territories.

One consequence has been the jihadi volunteers who have gone to Syria. Even if only a very small proportion of those who have gone return to Britain to cause harm, the training in terror techniques that they have received and the likelihood of their being further radicalised and brutalised by their experiences poses a very severe threat to the security of the British people.

In decades past, such dangerous plotting would be countered by traditional means: conducting surveillance on people or properties; installing bugs to eavesdrop on conversations, or talking to your informants or agents.

These approaches are still relevant but do not deal, entirely, with the new evolving picture. We have to come to terms with a world in which potential terrorists today may have no leaders, where they communicate using sophisticated encryption technology, and are just as much in contact, through the internet, with sympathisers in Yemen or Pakistan as they are with those in the UK.

Most people recognise that if actual or potential terrorists are to be apprehended, there is likely to be a considerably greater degree of intrusion into the privacy of the public by the security services than was required when our enemies were restricted to foreign governments.

Because of this some people have become increasingly anxious that our Intelligence Agencies are using the extensive technological capabilities now available through the Internet, to impose general surveillance of the public. This, it is alleged, has not been declared or approved by Parliament, and may be illegal.

It is, of course, not surprising that the Intelligence Agencies may possess capabilities about which the public have not been fully aware. This should not be controversial in itself – any intelligence agency would be rendered obsolete were all of its capabilities to become common knowledge.

For a few of the critics their concern is influenced by their presumption that the Intelligence Agencies have some sinister intent and are indifferent to the loss of privacy that their activities entail. Most, however, who express concern are more reasonable. They acknowledge that the Agencies seek to operate within the law but question whether any system of monitoring that is not targeted, exclusively, at known or suspected terrorists is either justifiable or necessary.

These anxieties were brought to a head in the debate surrounding the leaking of stolen intelligence documents by Edward Snowden. Snowden downloaded 1.2 million US top secret documents, including 58,000 relating to GCHQ.

There have been allegations against GCHQ, questioning, for example, whether they have introduced a system of general surveillance without proper authority or disclosure.

As the parliamentary body responsible for overseeing MI5, MI6, and GCHQ, I and my colleagues on the ISC have the responsibility to investigate these allegations.

We have begun a major and unprecedented enquiry into Privacy and Security involving our Intelligence Agencies. We have already received written evidence both from the Agencies and from private citizens, lobbies and NGOs. We will be taking oral evidence, some of it in public session, throughout the next few months.

It is against this background that I address this evening the central issue; are our Intelligence Agencies Public Servants or a Public Threat? In doing so I will address the following four central questions:

1. Are MI6, MI5 and GCHQ subject to the law , or are they permitted to act outside the law?

2. Are our Intelligence Agencies subject to satisfactory independent oversight in all that they do?

3. Even if the Agencies do comply with the law, is that law fit for purpose, and might, in any event, the law under which they operate, enable them to act in ways which are against the public interest?

4. Is there significant scope to increase the accountability of the Agencies to the public and to Parliament by greater transparency without doing serious damage to their operational effectiveness?

These are some of the issues being addressed by the ISC in its current investigation into Privacy and Security. That Inquiry will take several months to enable us to reach firm conclusions but I would wish to share with you our current thoughts and our priorities.

On the first question, it is worth reminding ourselves that Britain's Intelligence Agencies did not have any Act of Parliament to control their activities until as late as the 1990s. They were, of course, answerable to Ministers but only in an ill-defined and private manner. It was only as the Cold War came to an end, that the Agencies were placed on a statutory footing for the first time. The 1989 Security Services Act (for MI5) and the 1994 Intelligence Services Act (for MI6 and GCHQ) enshrined their responsibilities and protections in law.

Since 1994 they have had to operate within a very strict legal framework. They must comply with three basic guiding principles. First, their actions must be for a specific *lawful purpose*. Second, their actions must be *necessary*. Third, their actions must be *proportionate* - that is, they must be able to reconcile what is lawful with what is necessary. Unless they can meet all these requirements any use of their capabilities would be illegal.

None of the Agencies are free to use their powers indiscriminately. They are permitted to exercise their functions only in pursuit of the specific objectives set out for them in statute, which are first, the interests of national security; second, in support of the prevention or detection of serious crime; and, third, for the economic wellbeing of the United Kingdom where state security is involved. If an employee of any Agency uses any of his or her powers for any other reason, he or she is committing a crime and is liable to be prosecuted.

In addition to the legislation which sets out the Agencies statutory objectives, the Agencies must comply – in everything they do - with the 1998 Human Rights Act, which imposes a set of human rights obligations expressed in general terms. This includes an individual right to privacy which may only be interfered with to protect the safety of society as a whole.

In order to comply with the Human Rights Act, the 2000 Regulation of Investigatory Powers Act (or 'RIPA') outlines the detailed procedures with which the Agencies must comply when engaging in intrusive activity.

Part 1 of that Act outlines the requirement for a warrant application to the Secretary of State or other authorisation in order to monitor the contents of any communications.

These applications are no mere formality. The Agencies must make a detailed case, normally running to several pages. Warrants are subject to retrospective examination by Commissioners, who are, or have been, very senior judges, to check that applications are lawful and that the subsequent use of any warrant was consistent with those applications.

So there is, clearly, a substantial legal framework within which our Intelligence Agencies must operate if they are not to fall foul of the law.

That brings me to my second central question. Is there proper independent oversight to ensure that the Agencies observe the law and act in the public interest?

To meet that requirement, the 1994 Act also established the quasi-judicial Commissioners and the Intelligence and Security Committee to provide accountability that would ensure that the Agencies complied with their obligations.

Last year many were deeply concerned by suggestions in *The Guardian* that GCHQ might have, deliberately, attempted to circumvent its legal obligations by soliciting the NSA to provide them with intelligence material about British citizens that they were unable to obtain themselves because of the constraints of British law.

As the parliamentary body responsible for overseeing GCHQ, it was our duty to investigate these claims free from prior assumptions. We did so using the substantial new powers which the ISC has obtained under the 2013 Justice and Security Act.

We scrutinised GCHQ's access to the content of communications, the legal framework governing that access, and the arrangements GCHQ has with its overseas counterparts for sharing such information. Having consulted GCHQ's files, we were able to establish that in each and every case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in RIPA.

Unfortunately, the ISC has not always been able to report its conclusions with the same level of confidence. Until last year the ISC's powers were seriously restricted. Upon becoming Chairman of the ISC after the 2010 General Election I , and my colleagues,

initiated a review into the way the ISC then operated and the legislative framework within which it did so.

That review confirmed the inadequacies in the ISC's powers. Two issues stood out above all others as grounds for deep concern regarding the Committee's ability to reassure Parliament and the public that they could be confident with the conclusions of the ISC's Reports on the Agencies.

Firstly, under existing legislation, when conducting an investigation into Agency activity, the Committee could only 'request' the necessary documents and primary evidence from the Agencies. We had no legal right to insist on it being provided, and we could not be confident that any information provided was complete. I do not suggest that, in the past, the Agencies purposely obfuscated or tried to hinder our investigations. But an ISC investigation did not impose upon them the same statutory demands to provide all the relevant material as would be required, for example, for a court case. The Agencies have acknowledged that, in the past, they did not always identify documents for the ISC with the same rigour as they would if required to do so by a court order.

This vulnerability was exposed during a court case in relation to allegations of rendition and treatment of detainees. The ISC had published a report into the allegations but when the case went to trial, before a judge, further documentation emerged to which the ISC had not been given access. This did serious damage to confidence in the ISC's ability to conduct their investigations with the necessary rigour.

Secondly, while the ISC, since its formation in 1995, was formally responsible for scrutinising the Agencies' policy, resources and administration, it had been given no comparable responsibility for scrutinising Agency operations.

Operations are, of course, the most sensitive and important part of the Agencies' activities and are what give rise, from time to time, to most public concern, as we have seen with the Snowden allegations in regard to GCHQ.

In practice the ISC was able to oversee many aspects of Agency operations, but these were restricted to investigating a specific event at the request of the Prime Minister such as the London bombings of 2005, or allegations, such as rendition, that had surfaced in

the media . The ISC did not have the statutory right either to know about the operational capabilities of the Agencies in any systematic way, or the right to investigate operations at its own discretion.

We therefore strongly recommended fundamental reforms to the Government. The Government accepted our proposals and Parliament approved them in last year's Justice and Security Act.

The reforms to the ISC in the Act constituted a radical transformation of the Committee's powers. The ISC now has statutory responsibility for the retrospective oversight of MI6, MI5 and GCHQ operations for the first time. We now have the statutory right to ascertain, in detail, the agencies' capabilities in a systematic, as opposed to an ad hoc manner. The Agencies are now reporting to us on a quarterly basis with detailed information on their operational activities in the preceding period. GCHQ has been providing us with information on the full spectrum of their capabilities.

The ISC now also has statutory authority, under the Act, to *require* as opposed to *request* all the information, including the raw intelligence, it requires in order to conduct its investigations. The most radical change is that the ISC's own staff now have the right, and are using it, to go into the Agencies offices, access the files and , together with Agency staff , decide the files that will be given to the ISC, as opposed to having Agency staff doing it on our behalf. This is the first time external investigators from the ISC have been able to enjoy direct access to such sensitive material.

There have been further important reforms. The ISC is now also part of Parliament. Its staff will, shortly, become Parliamentary staff; it now reports directly to Parliament, and Parliament, not the Prime Minister, now has the last word on the Committee's membership. The Committee Chairman will no longer be appointed by the Prime Minister, but decided by the members of the Committee as to whom they think would be the best person for the job – whether from a Government or Opposition party.

Last but not least, the Committee's budget this year will be doubled, to around £1.3 million pounds a year. The number of its staff will rise commensurately. This is a significant increase in resources at a time of severe financial constraint.

These changes were initiated by the ISC and approved by Parliament before the Snowden story broke. The timing, however, has been very fortunate. We have, already, used these new powers in our investigation into the Prism allegations and the intelligence aspects of the murder of Drummer Lee Rigby; and are using them in our current Privacy and Security inquiry.

I turn now to my third question: even if the intelligence agencies do act in an entirely legal manner, does the existing law enable them, nevertheless, to act in ways which are, in practice, against the public interest, particularly in regard to the privacy of the citizen in this internet age?

This question goes to the heart of our current Inquiry on Privacy and Security. I cannot anticipate what our conclusions will be but I am able to share some of the major issues which we will be examining and taking evidence on.

These will include:

- Is there a balance that has to be made between privacy and security, as regards the interception of communications, or will it always be the case that the security of the public will, itself, be weakened if individual privacy is compromised?

-Should interception of communications by intelligence agencies be permitted only in regard to those individuals who are suspected of terrorist or criminal activities or should some bulk collection of data from a wider section of the public be permissible if it is done for the sole purpose of preventing terrorism and serious crime?

-Is there credible evidence as to the extent to which such bulk collection of data has made a significant contribution to the detection and prevention of terrorism and serious crime?

-Is the distinction in the legislation between the safeguards and procedures that must be applied as between communications data and the content of e-mails and the like, still valid and persuasive?

-Are the different requirements for interception by intelligence agencies of

communications entirely within the United Kingdom as compared to those to or from foreign addresses still valid?

-Are different legal safeguards, as regards interception of communications of British citizens living outside the United Kingdom compared to those who live within, justifiable?

This is far from an exhaustive list but will enable the unprecedented breadth of our Inquiry to be fully understood.

Finally, there is my fourth question for this evening. Is there scope for significantly greater transparency with regard to the capabilities and activities of the Intelligence Agencies without damaging their operational effectiveness? These, too, will be matters that we will be considering in our current Inquiry.

They include, for example:

-Should the Government explain much more clearly the legal basis for the Intelligence Agencies' activities including any bulk collection of data?

-Is it sensible or can it, on some occasions, be counter productive for the Government to persist in a "Do not Confirm, Do not Deny" policy to all intelligence queries?

-Should the existence of certain agency capabilities that have been widely reported in the Press be acknowledged, if they are true, when doing so might help reassure the public as to the unreliability of other allegations?

-Cannot much more be published as to the procedures that have to be gone through to get permission from the Secretary of State or other senior authority before interception is permitted?

It has been said that democracy is government by explanation. This might be true in respect of our Intelligence Agencies to a greater extent than has so far been assumed.

The distinction between intelligence agencies in democracies and those in authoritarian systems is crucially important.

Intelligence agencies exist in every state, both democratic and authoritarian, throughout the world. While they share certain things in common, we must never lose sight of the differences.

Intelligence agencies within authoritarian systems may wish to protect the public from terrorism and some types of serious crime. But their primary objective is the preservation of the regime they serve.

Unfortunately, the insidious use of language such as ‘mass surveillance’ and ‘Orwellian’ by many of Mr Snowden’s supporters to describe the actions of Western agencies blurs, unforgivably, the distinction between a system that uses the state to protect the people, and one that uses the state to protect itself against the people. It is ironic that Mr Snowden in the name of privacy and the rule of law , chose China and Russia from which to launch his attack on the United States.

Some people in Britain have pointed to the different reactions of the Press and the public to the Snowden revelations in the United States and Germany as evidence of some kind of uniquely British complacency. But this is to ignore the considerable political and historic differences within the free world.

For example, some cite President Obama’s response to the NSA allegations as an example for the UK to follow. But Obama’s most substantial promise has been to do away with the NSA’s own central database of American citizens’ telephone communications and to require the US agencies to access the information they need from the phone companies, themselves. That is, as it happens, precisely, the situation in the United Kingdom, at present. We have never had such a database in the first place, so there is no example, here, for the United Kingdom to follow.

People also cite Germany as an example of how we should respond. But for many Germans, references to interception by German intelligence agencies reminds them, inevitably, of their Nazi and Stasi experience. For the British, the comparable historic memory is Bletchley Park which shortened the war and ensured the preservation of our liberty. That should not make us complacent but it is a valid distinction.

We all live in a world in which there are occasional paradoxes. When a terrorist atrocity occurs, the majority of the public tends to ask why the Agencies knew so little about those who were responsible. When, however the surveillance activities of the Agencies are revealed, a smaller but vocal minority tends to ask why they need to know so much. We need to do a better job of recognising the competing demands we place upon the Agencies, and do more to establish a consensus as to how these demands can be reconciled.

Our Agencies are not, and do not wish to be ‘all-seeing’, nor ‘all-hearing’. Their capabilities have been designed to pursue their lawful, narrowly defined objectives.

True public servants operate with noble motivations, lawful authority, and subject to rigorous oversight. These are the values that distinguish public servants from a public threat. That is how those who work for our intelligence agencies see themselves. That is how most of the public see them. That has been my own experience seeing them at work over a number of years. It is in all our interests that that should remain their justified reputation in the Internet Age.

FINIS