STRAND GROUP: THE FIFTH SIR MICHAEL QUINLAN MEMORIAL LECTURE
14 JULY 2015

The Shifting Sands of the Intelligence and Security World: A Moral Sense

1 Introduction

I don't know how you arrived here this evening: perhaps you walked up Whitehall, past the Cenotaph, with its powerful commemoration of our war dead. Perhaps you walked up King Charles' steps, past the memorial at their foot to those murdered in the Bali bombing on the twelfth of October 2002; 202 people were killed, 27 of them British; those young Britons had an average age of 33 and the youngest was just 18 years old. And you probably came upstairs past the memorial to the staff of the Foreign and Commonwealth Office killed in line of duty.

I want to talk today about the environment in which a very special breed of public servant works, the crown servants in the security and intelligence services, those to whom such violent epoch-shaping events are calls to arms: this is a profession for those who decline to be bystanders. It is a profession for those who put themselves intellectually and emotionally, and sometimes physically, on the line, and who bear comparison with the finest of our armed forces.

I want to describe some of the changes in that environment over the decades through which I served, and to outline some of the challenges we have encountered, engaged with, overcome, and to explore how we have done so. I want to sketch a picture of the dilemmas we face today. And I want to colour in that sketch by painting a picture of how important ethics are in this world.

2 Quinlan relevance

When Doctor Jon Davis applied his force of personality and persuasion on me as to why I should give this lecture, building upon the moral pressure first exerted upon me with rapier-like refinement by Sir Kevin Tebbit, I confess my mental energy was concentrated upon establishing convincing reasons why I should not acquiesce - I was surely not worthy. Whilst I am certain that remains the case, I found myself bowing to the pressure when I researched some of the themes connected with Sir Michael Quinlan. I was particularly struck by the way he inserted ethics into the equation.

Our intelligence and security agencies operate within a British legal framework. More of that in a moment. But my overriding conclusion after three decades in the business is that the law itself is just one of the compass bearings that guides our work, whether day to day or year on year, tactically, operationally or strategically as the military might put it. As important is the concept of ethics, an innate sense of right and wrong, the complex set of interlocking values that tell me that there are some things I should, and some things I shouldn't do, irrespective of the fact that they may be legal, and irrespective of the fact that other people might or might not do them. One of Michael Quinlan's contributions was to make the point to us all that we have to think about this. And for me this ethical sense sits alongside the notion of a moral responsibility to get involved, to seek to make a difference, not to be a passive bystander. And with this comes self-respect: an ability to look myself in the mirror each morning.

I am giving this lecture in order to share this perspective with this invited audience. I am not seeking headlines, and I am not even trying to set the record straight in any defensive sense, tempting though that might appear to some. There is a notion of public service as practised by the crown servants in the intelligence and security services of the United Kingdom that I want to explore, a service that goes beyond the ordinary and in fact often approaches the extraordinary, that displays itself through a remarkable selflessness and dedication.

3 What is our role?

If you alight from the tube at the front end of the Bakerloo line platform at Piccadilly Circus underground station, you would do well to 'Mind The Gap.' There is an alarming gap of some 12 to 18 inches which is just the right size for a large boot to disappear down.

The job of the United Kingdom's intelligence and security agencies is to reduce the size of the gap between ignorance and knowledge, between unwittingness and readiness, between misapprehension and comprehension. They do so for our Prime Minister and other Secretaries of State; for our admirals, generals and air chief marshals, in fact for our military at all ranks as they conduct military operations; for our scientists and engineers researching our future weapons capabilities and anticipating those which might be deployed by potential adversaries; for our security professionals and law enforcement agencies countering terrorism and serious crime; for our foreign policy experts seeking to defuse international crises and to promote the principles and values in which we believe; for our government economists as they seek to chart a course through future uncertainties; for our cyber security gurus as they build and promote better protection and defence of our data networks whether governmental, industrial or commercial, academic or personal.

And whilst I speak from the perspective of an intelligence and security professional, or at least as a former leader of an intelligence and security organisation, I believe some of the factors and themes I hope to illuminate are relevant in wider spheres of public service and policy.

4 Our Focus

It would be straightforward to connect the existence of the intelligence and security agencies with statecraft, with regional influence, with the anticipation of and if possible avoidance of conflict, or - in the case of its realisation - with its rapid resolution, if necessary through actively supporting those engaged in violent military endeavour deemed to be 'just.'

In 2009, the British intelligence community celebrated the centenary of its establishment in unbroken lineage to the current community. We at GCHQ had to wait a little longer until we were able to celebrate the centenary of the establishment of the first coherent Signals Intelligence organisations from which we were descended - 2014, a hundred years after the First Sea Lord, Winston Churchill, issued in November of 1914 a Charter.

That Charter prescribed the operating model in which Room 40, the section in the Admiralty which had started producing intelligence from intercepted and decrypted messages, would operate. Churchill oversaw the birth of British Sigint, and was instrumental in the creation in 1919 of GCHQ, under its former name of GC&CS, the Government Code and Cypher School.

It is primarily from this GCHQ perspective that I shall speak. I will talk about the intelligence target sets against which we have worked over the intervening decades - the potential sources of the intelligence we are charged by a formal requirements and priority process to collect; the communications environment in which those targets operated and on which Siginters - those engaged in this trade - therefore worked assiduously and relentlessly; the changes in technology that both challenged and fuelled our capacity to make the critical difference we sought, for the moral reasons of which I spoke earlier; the community structures around our work, including mandate and oversight; the tightening of linkages between intelligence - the work of the poacher, and security - the work of the gamekeeper. And I shall wax lyrical about the transformation in leadership and followership up, down and across our modern workforce.

First I want to explain an important professional trait inherent in the workforces of the three intelligence and security agencies. Her Majesty The Queen, when she unveiled the memorial at Bletchley Park, described the people who worked there as problem solvers. She said:

"At heart we have always been a nation of problem solvers. This natural aptitude was taken to new heights by the emergency of war, showing that necessity is indeed the mother of invention, and that battles can be won, and many lives saved, by using brainpower as well as firepower; deliberation as well as force."

We keep alive and vibrant that aptitude and we celebrate it. On the occasion of The Queen's Diamond Jubilee, GCHQ sent our congratulations in the form of a Loyal Address in code. For the cipher spotters amongst you it was the 1952 edition of the British Inter-Departmental Codebook and for the re-encipherment key it used the four figures One Nine Five Two. Subsequently we received a reply from Buckingham Palace in the same code. This affirmation - the fact that The Queen responded in code - resonated deeply within our Community and across our close Commonwealth allies, royal recognition that how we see and value ourselves is appreciated by one who has done service for well over half GCHQ's history, who is in fact the individual in the allied community who has been receiving intelligence material for the longest period of time.

Problem solving is part of what we do. It also underpins a lot of what we need to do before we can even get at our intelligence targets' communications: how do we work out which of the myriad new apps appearing every month might be the one which the terrorist will take up? How do we find the terrorist amidst the channels of communications available to him? How do we even start when we find that an intelligence target's communications have been encrypted? And how do we do all of this and stay firmly within the law?

This intellectual desire to understand <u>why</u> our target is doing what he or she is doing, to contextualise his or her communications, is as much part of Sigint DNA as the abiding interest in the development of new communication technology.

5 The Intelligence Target Set

a. Actual or potential aggressor Nation States …

Actual or potential aggressor Nation States made up the bread and butter of the Sigint work of the Government Code and Cypher School and its predecessor organisations, and of GCHQ for much of the last century. So you will find accounts of the work against Germany and its allies during the first world war; the extraordinary story before and during World War Two on ENIGMA and in due course LORENZ is well told from the perspective of Bletchley Park and its outstations working against the Axis powers; and it is a fair assumption that the Warsaw Pact was the primary raison d'être of GCHQ in the post war years until the Soviet Union's disintegration in the period after 1989.

At the same time it was in these years of prolonged or frozen conflict that the equally vital work of securing our own networks and communications of national importance came to the fore - a theme to which I shall return when I explore the modern-day concept of cyber security, for there is nothing new under the sun.

b. … and the growth of Transnational targets

After the split-up of the Soviet Union and its allies there was a peace dividend to be had: forward intelligence bases were dis-established and closed; the term 'rest of the world' ceased to sound like the Cinderella mission; transnational target sets such as narcotics, financial crime, people trafficking, proliferation, terrorism took on prominence. 1991 was a doubly significant year for GCHQ: the Soviet Union fell apart, and the World Wide Web was established.

To be sure the military interventions of the first half of the 90s that we saw in Kuwait and Iraq under Operation GRANBY and in the Balkans under UN mandate as UNPROFOR fully engaged the intelligence apparatus. But there was nevertheless a balkanisation of intelligence collection and analysis, with no 'main effort' - no principal priority verging on the existential - clearly rippling through the fabric of our community.

c. Blindsided

That changed in 2001 with the horrific events of September the 11th and subsequent military campaigns in Iraq and in Afghanistan. Our American allies used a term that in retrospect at least appeared ill-chosen - the Global War on Terror - but these were years of concerted, sustained effort, of tight integration with our armed forces and organic support to military operations at all levels. In my experience the closeness of that partnership was exceptional, carried out at tempo, scale and with precision.

Even then however it was temptingly easy to think of counter-terrorism as an activity that took place 'upstream' from the UK, that played out in landscapes far away, where the fight had been taken to the adversary.

On the 7th of July 2005 that too changed as we felt physically sick that we had been struck on home soil in four concerted acts that wreaked death, maiming and horror on innocent citizens, visitors, tourists in London. Counter-terrorism became the main effort and a moral driver for the workforces of the security and intelligence community. Just seven days ago on the tenth anniversary, we marvelled at the fortitude and moral strength of survivors, of relatives and friends of those who died, of rescuers: inspiring, brave, forgiving and strong. That unifying strength ten years on finds parallels in the resolve felt across the intelligence and security community ten years ago.

It is a matter of great pride that in the years since 2005 only one terrorist murder has taken place on the soil of Great Britain, that of Drummer Lee Rigby in Woolwich in

May 2013. It is not chance that this is the case, but the consequence of committed, assiduous, painstaking analysis, discovery and disruption of violent extremist planning, of online radicalisation, even of late stage preparations for attacks. It is a matter of public record that multiple plots have been thwarted. Investigative and operational work took place in MI5, in GCHQ and MI6, in the Joint Terrorism Analysis Centre JTAC, in police forces across Britain. Assessments and interventions were founded upon fine-grain intelligence work which drove precision actions. Intelligence work is rarely straightforward and seldom at the easy end of the spectrum: even before our sources and methods are discussed in public, and picked apart under a microscope, this is metaphorically back-breaking work, chiselling away at an enormous quarry in pursuit of a potentially rewarding seam of ore that might illuminate suspicious activity, that might trigger a lead that can be followed up.

d. Then Cyber Security

The UK's first National Cyber Security Strategy was published in June 2009; then the next government produced a new strategy in November 2011 and - in recognition of Cyber as a Tier One risk - created and resourced a cross-government programme with four objectives:

- to make the UK one of the most secure places in the world to do business in cyberspace
- to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace
- to help shape an open, vibrant and stable cyberspace that supports open societies,
- and to build the UK's cyber security knowledge, skills and capability.

I believe this was a national game-changer, establishing the UK as an international thought-leader on cyber; generating the concept of a national ecosystem engaging government, industry and academia with shared responsibility for best practice and joint leadership; creating fora for sharing knowledge of attacks, compromises and mitigations. It was and is a subject that quite rightly engages Ministers and business leaders, and one where today's best practice will inevitably face the charge of inadequacy tomorrow.

It has also been an institutional game changer for GCHQ, forcing us to forge qualitatively different partnerships with specialist industry; to work with the Department of Business, Innovation and Skills and with Research Councils to establish academic centres of excellence for cyber security research; to develop new international partnerships beyond the traditional Five Eyes - American, Australian,British, Canadian and New Zealand cryptologic allies - in order to build coalitions to detect and defend in cyber space.

e. Libya

In 2011 there was a short, sharp and highly successful military campaign in Libya, one where technical intelligence provided decisive support at tempo and with precision - not the first time I have used that description. This built on the hard-earned lessons of Iraq and Afghanistan and was a model of intelligence support to the warfighter.

f. Aggression to the east of Europe

But in early 2014 military adventurism on the eastern borders of Europe reminded us that hard-won insights into the military capabilities, tactical manoeuvres and operational

effectiveness of global powers are quickly lost if not sustained, that the saturation of intelligence sensors that existed some decades ago is not one which can be rebuilt overnight, and that the deep analytic expertise built up over decades is not a quality that can be mothballed and simply deployed when needed.

And the downing of MH17 reminds us that there are terrible mistakes made in the fog of war that shatter the lives of innocents who have no skin in conflicts. Once again I hear that moral imperative calling: to engage in discovering what is happening, in identifying the attendant risks, in creating understanding and knowledge of situations so as to avert harm and mitigate damage.

g. Ungoverned space

And now we sit here just three weeks after an act of violence on a tourist beach in Tunisia, an act ironically both indiscriminate yet targeted. Even more Britons murdered than in the dreadful Bali attack of 2002 that I mentioned at the outset. It serves as a reminder that we must now recognise that this intelligence and security community faces large-scale challenges that may be transnational or may be nation state-derived - double jeopardy. What they have in common is the capacity to create persistent, sustained instability as the backdrop to government's duty to seek to protect its citizens and its interests at home and abroad.

6 The technological environment inhabited by intelligence targets…

I've spent some time talking at a macro level about the 'target sets' that this community is charged with covering. Let me explore a little the technological environment in which those intelligence targets communicate.

At its most elegant, Sigint would search for and then intercept only a communication of interest, process it including subjecting it to decryption if necessary, and render it into intelligible form whereupon - if intelligence-worthy - a report would be produced for an authorised reader.

Sigint has always been a matter of prioritisation and of reduction: and there are obvious parallels in government's potentially intrusive powers going as far back as the First World War where some 100 million telegrams went through censorship - nobody could read them all, nobody wanted to read them all.

As I have said elsewhere, the concept of the specific frequency dedicated to a user of interest, whether the communication content was carried *en clair* or in decryptable or unreadable cipher, allowed immediate focus and tailored collection.

Expressed at its simplest, Sigint needs to understand the technologies available to our adversaries, to comprehend how our targets interact with those technologies, and what that means in terms of the global telecommunications network. Our predecessors in the First and Second World War wouldn't have used that vocabulary but they would have recognised the underlying thinking: the network is our environment and we need to understand it first.

But moving beyond old-fashioned wireless to cable technologies, or to multichannel and spread spectrum, from analogue to digital communication created something like a technological arms race: how could we filter into scope in near real-time communications

of interest, when simply finding the communications in an ever more complicated environment became harder and harder. And nowhere is this more evident than on the Internet.

The Internet represents an enormous soup where oftentimes it is patterns of usage that are the only way of identifying those communications of interest. Bulk access is nothing new - look back to the declassified pre-war histories of Sigint for their accounts of cable exploitation.

The trick is to go from that bulk access to fine grain selection and consequent analysis as quickly and surgically as possible.

Actual or potential state-level adversaries of interest, weapons of mass destruction proliferators, narcotics traffickers, financial criminals, terrorists, child exploiters, destructive hackers all swim in this soup. As of course do we - as society, as government, as business, as academic and research institutions.

7 … and by ourselves

And so the trick is also to secure our own networks and data of importance, which means measuring the value of that data or the network on which it is carried; assessing the impact of a breach of its confidentiality, of its integrity or of its availability; understanding where it is stored, who is charged with protecting it and how, and who has access to it.

Put all this together and you arrive at the concept of Cyber Security. It is the domain where the science of security comes together with the art of penetration so that the knowledge inherent in one discipline offers advantage in the other, allowing a ladder effect whereby the underlying capabilities - on the one hand to secure one's own communications and on the other to arrive at the possibility of exploitation of a valid target's communications - ratchet up together.

Pause for a moment to reflect: it is impossible to provide a defensive cyber security apparatus without operating first at the level of bulk in order then to winnow out the chaff in order to end up with the questionable streams of ones and noughts that represent malware or phishing in a digital environment.

It is the aggregation of data and the integration of analytic methods that offers the possibility - and it is a matter of ratios and fractional probabilities - yes, the possibility of detection and prevention of the uncertain or dangerous, the untrustworthy or corrupted, and thereby the protection of systems and their data.

8 Tempo

If we think about the journey from that deep expertise in understanding the highways and byways of a nation state's communications during wars or conflicts, frozen or otherwise, to this Internet world, a new factor becomes evident - that of tempo. Tempo where actionable intelligence is required by an operational user in minutes or even seconds. Note my use of the word 'actionable' - much of the intelligence generated by Bletchley Park in World War Two was strategically useful and actionable in that sense, operationally valuable in the sense of being able to influence large-scale engagements, but tactically a non-starter for fear of jeopardising the source - the golden eggs and the geese that laid them, as Winston Churchill almost put it.

Perhaps at GCHQ we cut our teeth in generating actionable intelligence in our support to law enforcement, exercising our mandate to support the prevention and detection of serious crime. We must surely give most credit for the transformation in the supply of actionable intelligence to the operational teams involved in supporting the operations of our armed forces in Iraq and Afghanistan: giving the critical advantage in real time to soldiers in conflict. And our counter terrorist work depends on that same tradecraft and mentality. But actually the ethos of delivering intelligence which can be effective in preventing harm or forming the basis for positive action, at tempo and with precision, is a quality that permeates the work of the intelligence and security agencies across all missions, across the board. It has been and will continue to be a game changer. And the beauty of its correct application is that by dint of that forensic focus on the end result and how to get there as efficiently as possible, it also supports the principle of privacy for the many, for the vast majority, as analysts drill down to the vital seam.

And consider the defensive side of cyber security - it is no use providing delayed commentary on cyber attack - edited highlights after the event don't really work. This is a contest that has to be waged in real time where action to isolate and quarantine, or to validate and permit, needs to take place at net speed, not after the event.

And with this tempo, the need to be able to act and react more and more quickly, comes the imperative for a workforce which is aware in the heat of the moment of the constraints on and consequences of their ability to act, as aware as a soldier in battle is of his rules of engagement,- of what they might and might not do. But, because of the infinite variety of ways in which a target communication might travel over the world wide web, our rules of engagement will have to be generic in many cases: so we need an operational workforce which is not just technically but also legally and equally ethically clued-up: cautious and scrupulous in applying the methods that the law allows them to use and yet operating at the tempo demanded by military, counter-terrorist, law enforcement and cyber security operations.

In the anarchic chaos of the Internet those who search it for intelligence in support of national security and the prevention and detection of serious crime are not cowboys: they may be operating in the Wild West but they act as the sheriffs and marshals.

9 Mission Command

And this tempo and the need to get it right first time leads me to draw out a workforce transformation which has been a tremendous force multiplier. The military have the concept of ‘mission command’ - setting out the required outcome, the constraints which apply and the resources available, but then leaving the ‘how’ to those charged with delivery of the task. This promotes freedom and speed of action.

In an Internet world it is not possible for the leadership at the top to do more than set the direction: the speed of activity requires decentralised command so collectors and analysts can operate within the time cycle of the communications they are seeking to detect and to exploit or perhaps to disrupt. It means letting go and allowing the specialists to use their professional instincts, to seize the moment, to be opportunistic when opportunities emerge unexpectedly, to act spontaneously, to grasp the initiative in cyberspace - but in all of this to do so within the bounds of law and policy. It is my view that the intuition at the heart of this ebb and flow of individual decision-making is founded upon an ethical awareness, indeed upon a personal interpretation of what is right and what is wrong which is more subtle than the mandates and strictures of law. The operator’s ethical sense plays

as powerful a part in creating the conditions for success as does the specialist capability of the operator, and success can only be categorised as such if the aim is achieved lawfully.

In a complex, uncertain, often chaotic communications environment it is this concept of mission command, of empowered well-trained, well-skilled individuals acting as a team in pursuit of a common goal, without prescriptive instruction, that has to apply: I can think of no other command system of tasking and achievement that could be successful. And as I have said, that success depends not just upon specialist skills but upon the ethical sense developed by operators as a result of experience, of open discussion and argument, and of reflective thought. With that grounding they can take the responsibility to act within the tempo that the cyber domain demands.

Of course we have controls in the shape of logs, checks, audits and reviews, but we start from the distinct advantage that the operators in the workforce are driven by a great sense of responsibility within an ethical framework.

10 Leadership

A few words on leadership. In an era where the workforce has at its heart a great chunk of the Internet generation, a generation that really does not react well to being told how to do something and would much rather make up its own mind once the intent is clear, the senior leader's role becomes very different.

Some of it is about setting out that intent, the desired outcome penetratingly captured and punchily expressed, to foster mutual understanding and a basic set of assumptions on which to fall back in times of confusion or overwhelming pressure. Some of it is about ensuring unity of effort. Direction of travel too maybe. But also I think a steward for the ethics that need to apply, fostering open debate where concerns are raised, tackling awkward issues, including upwards if necessary.

And there is another role which I might start to describe through an anecdote: One colleague at GCHQ said that seeing the three agency heads in front of the public evidence session of the Intelligence and Security Committee was "like watching our last line of defence—and it held just like we knew it would". There is a role here around saying plainly and if necessary publicly to those charged (by parliamentary statute) with oversight that our workforce has nothing to apologise for, that what we do is lawful, proportionate, necessary and effective, that we hold our heads high.

But much of that explanation needs to be done in secret and that private exposition does indeed take place. Our intelligence agencies are a lever of power. They are different from the Armed Forces, and from other public services, because they work in secret. But they need to be completely transparent to the independent overseers who in turn preserve the secrecy of what is done lawfully.

11 Transparency and the Press

Exploding around the well-intended and I fervently believe authentic efforts to develop transparency by leaders of organisations such as the one of which I was the Director, comes the overwhelming force that is the attention of the media. At one extreme this sometimes seems to represent itself as a distrust in the competence of those who have

chosen to devote their careers to public service; at another it can seem to be an ideological assault on a form of crown service that seems to those within it as the most moral of careers, as a ‘noble profession’ as I have termed it elsewhere. It is easy to exaggerate a sense of injustice when on the receiving end.

The other factor of course is the tempo which media attention brings to consideration of any issue which might merit controversy. Inevitably real or imagined controversy attracts political attention; just as inevitably that political attention demands to be fed - and fed instantly. There are some issues that deserve a pause, a reflection, perhaps no more than a quizzical eyebrow.

In June 2013 when certain allegations burst on the scene it was the cool head of the then Secretary of State for Foreign and Commonwealth Affairs which prevailed - setting out in parliament the lawfulness, proportionality and necessity of GCHQ’s intelligence operations. An authentic statement underpinned by a powerful, energetic sense of accountability for the operations of GCHQ and by a rigorous, disciplined record of authorisation that is one of the features of the British legal and policy systems surrounding the intelligence and security agencies of which we should be extremely proud.

As a consequence the overwhelming innate urge to deny, or to seek to refute was one which was resisted. Frustrating though the ‘Neither Confirm Nor Deny’ doctrine is - often to those espousing it as much as to those assailing it - it exists for a reason: to protect sources and methods of intelligence collection which once exposed and confirmed are burnt for good. That doctrine does not exist to save embarrassment or to protect organisations from accusations of grubby practice. And indeed it cannot be deployed to do so.

The hardest aspect of such drama is the inability to speak up, the firmly buttoned lip. As the leader of an agency which prides itself on its integrity of analysis, on the fundamental commitment to do the due diligence before reaching a conclusion based on intelligence collection, not merely to represent as a truth something that is in fact simply a leap of faith, to avoid any temptation to take the shortest route between two corners of a triangle when provability demands analysis that goes the long way round - it is a matter of shock to see misrepresented conclusions or the darkest possible interpretation placed upon methods of intelligence work applied unstintingly for the greater good.

And as the leader of an agency composed of people whose integrity has been questioned but whose integrity of analysis in their day to day work is at the heart of their identity, this is hard to take: hard for me, I might just say, and even harder for the immense majority of staff who are never going to have an opportunity like this to tell their side of this story.

Transparency can be a two-edged sword. This is a modern phenomenon: GCHQ's existence was not even avowed until 1983, and the Intelligence Services Act itself dates only from 1994. We enjoyed, in every sense of the word, a secret existence.

But as the level of intrusiveness of what we do increases, it becomes more and more necessary that there should be an understanding of what the capabilities entrusted to us by law actually enable us to do.

We need to explain, insofar as a secret intelligence organisation can explain without compromising its capabilities, to the British public what we are for and how, legally, we do our business.

And that's why we talk to the press: tens of millions of our fellow citizens access news through the media every day, and if our fellow citizens are going to understand not the detail of what we do, but why there is a GCHQ and how it is working, in accordance with the law, to protect them and their liberties, it is necessary we should deal proactively with the press to enable us to counter the myths about our capabilities and what they were used for.

A British public which is educated about Sigint and the generic capabilities and contributions of GCHQ, is not a threat to our activities; on the contrary, it provides a democratic safeguard which ensures that intelligence activities aren't just the province of the man in Whitehall who knows best.

But in this era of transparency, of reviews which are then published - rightly in my view - with the least amount of redaction possible, it must begin to beg the question as to whether secret intelligence work is still a reality, or whether secrets can remain 'secret' to the extent anticipated when they were classified as such in the first place.

I happen to think - though I would say this wouldn't I? - that the judgement on what is and is not secret should rest with government, with the duly elected government held to account by parliament. Not with the press. The government is elected and, notwithstanding the public's natural inclination to object to the unpopular actions or policies of government, those in government remain our elected representatives. The shining torch of the press, however deftly wielded, is not an elected tool, nor one trained in making judgements around the fragile equities of intelligence sources and methods, and the full facts are not at their disposal. Decisions on national security lie with government.

But this is a fine judgement and it is why, separate from all the internal mechanisms we have, we have had the mechanism of the Defence Press and Broadcasting Advisory Committee, commonly known as the 'D Notice Committee'. I have seen much nonsense written about this committee - my favourite being its description as a means of fascist censorship - that could not be further from the truth. It is a body made up of media representatives and government, with a small staff. Its secretariat exists so that matters of potential sensitivity can be tested privately and responsibly. It is not a means of muzzling the press but of allowing responsible and constructive influence to be brought to bear. from both sides. I quote from the government website:

"The Defence, Press and Broadcasting Advisory Committee (DPBAC) oversees a voluntary code which operates between the UK Government departments which have responsibilities for national security and the media. It uses the Defence Advisory (DA)-Notice System as its vehicle. The objective of the DA-Notice System is to prevent inadvertent public disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives."

Sounds remarkably sensible to me. It is a voluntary code, to which newspapers and broadcasters choose to sign up, it exists for a purpose, if necessary it should be further demystified and publicised, and it should be used.

Let me come back to leadership: under what can seem a tumultuous assault, it is tremendously sustaining to feel the indignation and pride, the commitment and tenacity of the workforce who are counting on you to set the record straight as best one can and to

keep stakeholders onside. The assault on integrity brought into stark relief for me the fact that the moral code of GCHQ staff was as much a part of their identity as their sexuality or spirituality or physicality.

13 National Structures

In 1994, Sir Michael Quinlan undertook a review of the intelligence services. It is a deceptively common-sense summary of factors and recommendations that we now take utterly for granted:

- setting out the link between requirements for intelligence and the resources which then need to be allocated - especially important for GCHQ because we need not just to allocate existing capability to current requirements but also to invest in new general capabilities that future requirements will call for.

- recommending tighter, more rigorous interaction between the customers for intelligence and the producing agencies: the idea being that better understanding of intelligence capabilities would drive better-focused requirements, which would in turn result in better quality intelligence, better meeting the needs of those intelligence readers.

- Stipulating the need for annual performance reports from each agency, later enshrined in the Intelligence Services Act that year.

- Taking the trouble to explain why secret intelligence is necessary: to offset gaps, uncertainties or distortions in overt information, in order to advance the national interest. And in particular, to enable national forces to prevail in conflict, with minimum loss.

- And he even recognised that it was increasingly likely that future military action would require politically sensitive and accurate application in complex situations, rather than heavy firepower, tending therefore to increase the value of intelligence.

- He set out the case for a peace dividend, for a major drawdown of effort around the Russian target, even postulating hypothetical 40% cuts. I do wonder rather wickedly what he would make of current geopolitics around Russia, although being Quinlan there is probably a footnote somewhere, presaging exactly the current situation!

His was the first serious study of the post-Cold War intelligence world. His statement of the case is both masterly and foresighted. It is also I think the last major review of the intelligence community before the major changes effected by the new Coalition government in May 2010, this time changes to the centre rather than to the agencies themselves, although these changes were pivotally focused upon the ultimate cohesion, purpose and outcomes of the work of the agencies.

The new government established a National Security Council and the National Security Adviser post, along with an underpinning National Security Secretariat.

In my view that National Security Council structure was even more important than the National Security Risk Register and National Security Strategy that were then drawn up over the succeeding months along with the Strategic Defence and Security Review prior to the Comprehensive Spending Review. It brought together the Prime Minister in the chair along with the principal Secretaries of State charged with national security issues: the Foreign, Home, Defence and International Development Secretaries, the Chancellor,

the Chief of the Defence Staff, the National Security Adviser, the three agency heads and the Chairman of the Joint Intelligence Committee, as well as other Cabinet members as required. It offered a weekly - sometimes more frequently than weekly - opportunity to debate foreign and defence policy issues, terrorism and cyber security, regional crises and global trends.

Inevitably the temptation is that it becomes too near-term in focus - diligent, careful, highly competent attention to the issues *du jour,* at the expense of a strategic look ahead. Given the spate of crises over the last 5 years it would be almost perverse if there had not been a forensic focus on current events - the need to act, the right course of action, the review of action taken - rather than where we might want to be in some years' time. The risk however is that consideration of hard-nosed national interest takes second place to exploration of immediate palliatives.

But make no mistake, the creation of the National Security Council is fundamental to securing value from this elite community of intelligence officers and security professionals. Of course the outputs of the three secret agencies are consumed tactically in volume and detail by a range of operational customers at home and abroad. And it is important to affirm the value of the myriad pieces of the jigsaw, none of them earth-shattering in its own right, which nevertheless when joined together reveal a fundamental truth about a nuclear weaponisation programme, or the readiness of a nation's armed forces, or the intent of a terrorist group, or the development of a new transnational criminal grouping.

But it is the ability to inform the top leadership of government, to allow them to shape strategy, policy and operations with knowledge that makes intelligence such a priceless asset. The Catalan architect Gaudi worked with architecture as a means of drawing out light in a balanced way; intelligence is a means of drawing out understanding of complexity and ambiguity and therefore shaping the knowledge to develop and select courses of action for national advantage (which can often mean avoiding national disadvantage).

With the development of a powerful cross-government body such as the National Security Council, and its 4 star-equivalent officials' committee both preparing for and taking instructions from the PM's meeting, it is easy to see how Cabinet Office secretariats might enlarge and accrete power to themselves. Instead we should look for leaner staffing at the centre, a premium on expertise in the producing agencies, and greater responsibility for the departments of state charged with developing policies and operations. We should place a prize on the intelligence producers at the nation's disposal and equally on the professionals who keep our streets and networks safe.

It's also a mistake to confuse 'national security' with foreign policy. As I sought to explain earlier, the national security environment is no longer one that might be restricted to diplomatic wrangles or tempering ostentatious flexing of military muscles. It is one that is transformed by the transnational and the asymmetric.

14 The Cyber dimension

And surely there is no more asymmetric phenomenon than cyber with its capacity for transnational effect; for deception, denial and disruption, and even destruction; for criminality and espionage; for protest and covert influence. Protection and defence are activities in a constant state of flux, with advantage passing back and forth between those who would exploit and those who detect, discover and counter. Skirmishing in cyberspace is

constant. And it is the arena where muscles can be flexed covertly or ostentatiously, with a false flag or no attribution at all, with temporary or lasting effect.

There are few if any disputes or conflicts which do not play out in the parallel world of cyberspace, even while diplomatic or military manoeuvring may be the more public focus of attention.

It is a domain where smart adversaries have the advantage of seeking and securing hostile effect by acting against proxy targets - countries other than their primary target, because they are seen as an easier option; sectors other than national leadership, defence resources or the instruments of foreign policy - because (like the Heineken advert most of this audience won't remember) cyber reaches the parts that other weapons do not reach, it finds out the areas where strategic resilience is lacking.

Cyber maturity will define alliances and coalitions of the future - weaker, vulnerable players in cyberspace will be seen as liabilities not as assets: why would countries which represent a soft underbelly, a vector for penetration by an adversary, be tolerated within a greater international endeavour?

It is of course a domain where sophisticated criminality is now rife, where new product releases of malware are diligently managed as they are made available in a covert world of mutually beneficial illegal commerciality, where if an e-attack fails against one victim it is simply tried against another, and another, and another.

And it bears a reminder that this is not just an IT issue: physical security plays a part, but so, also more strikingly, does personnel security. What is termed the Insider Threat is a primary vector of vulnerability; it has moved from a niche issue to a central issue: awareness of and consequent judgement around individual privileges, of potential or actual accesses by individuals to data, of their consequent actions with respect to that data - all this has become a fundamental management and compliance issue.

So the security mission has moved to centre stage - no longer secondary - alongside the intelligence mission, and at the apogee of intelligence work and of security work, there is a virtuous circle, mutually beneficial corollaries, as I set out at the start of this lecture.

And that security work is of course not the preserve of government. Industry and academia have as great, perhaps even greater, roles to play. Those roles, just like that of government, have to be exercised with responsibility. There need to be fora for dialogue and mechanisms whereby law enforcement under properly authorised conditions can carry out its own role with the assistance of communications and applications providers - and that assistance needs self-evidently to be on a confidential basis. I said the UK needs to be the best place to do business, but equally we want it to be the worst place for terrorists and paedophiles in terms of their capacity to profit from the online environment. These solutions must be capable of operating at the speed required to defeat the tools of anonymisation used by terrorists and other criminals.

There is not a straightforward road to this happy state in an epoch where commercial organisations operate on the currently prevailing transnational or even supra-national basis.

The seismic shift that cyber represents to the intelligence and security world presents challenges to the leadership in that world. I was asked the other day what good leadership looks like in the cyber domain and I would offer three aspects to reflect upon:

- first and foremost it means instituting and sustaining intelligent partnerships, encouraging and shaping the network of relationships required for a successful collective approach: this is not a domain where any single player can truly thrive. Traditional international partnerships need to be reshaped for a cyber era, with new partners enjoying geographic or technological advantage invited to a common cause. Partnerships across government are indispensable. And as I have said, partnering between government, industry and academia is now cardinal.

- it means living with ambiguity: often cyber presents complexities which take time to resolve with any degree of certainty, where things are not always what they seem, where the thirst for quick answers needs to be resisted. Particularly where cyber attacks are concerned, there is an impulse to attribute - this is a distraction from the harder-edged questions that need attention - such as the degree of resilience which was meant to be in place, or the vector of penetration, or the speed of mitigation, or the likelihood of full recovery against the risk of reinfection.

- and increasingly it means being prepared to indulge in or at the very least stimulate thought leadership.

15 Back to Ethics

When I was half way through this draft, which I had titled 'The Shifting Sands of the Intelligence and Security World' I found myself adding a subtitle: "A Moral Sense".

I want to finish on this theme, building on what I hope you have detected throughout. We are crown servants: that means we take our instructions from the elected representatives of the people and while we can advise - and it is our duty to advise - it is just as much our duty to accept that ministers will either accept or reject our advice and we will then do as we're told.

Echoing my earlier comments, decisions on what is and is not secret do not lie with individuals with moral qualms: there are avenues for such individuals to use and to afford those individuals at best satisfaction, at least a hearing and explanation. I believe utterly that moral dilemmas should be aired, explored and used to afford clarity and where appropriate change for the better.

If we have an issue with that we can resign. Conscience is hugely important in this. But it must be informed conscience - not brandishing conscience as an opt-out, as some sort of get-out-of-jail-free card which allows you to do whatever you want, as long as you believe that it's right for you. You have to inform your conscience: if you disagree innately with something but that something is legal, then you should according to conscience stop doing it - and that would mean resignation and perhaps then campaigning to have the law changed. But your conscience-based view does not make the activity with which you disagree wrong - and if you disrupt that legal activity, that makes your action wrong. But my main point is around an uninformed conscience - individuals who choose to leak classified material can make misplaced decisions about proportionality because their understanding was incomplete, or selectively applied, or because they did not take the trouble to re-

search, debate, challenge and argue, through the established processes which exist: processes which exist not in order to constrain or muzzle dissent, but because those challenges can initiate improvement and better application.

And happily the overwhelming majority of our staff have an ethical code that guides them on exactly the right lines.

16 Conclusion

Crown service needs to attract the very best - in skill and ethos - from society. Crown servants are not going to retire as comfortably as they might have done in times past. They are in my experience not for the most part independently wealthy. And for a sizeable proportion, their skills and equally their attributes are eminently saleable and can command significantly higher salaries than those available in the agencies.

And some do leave, because the money they can earn outside gives them better options for their families' futures. Some GCHQ staff for example leave because they are frustrated that GCHQ - part of the Public Service - can't be like a public company. Some leave because they are ground down by the awfulness of what they learn people are capable of doing to other people. But most don't, and some of those who leave will come back. Whether they are the ones with high-end marketable skills or the ones whose job it is to make sure the wheels keep turning, staff at GCHQ and at the other intelligence and security agencies have chosen to be part of making history, not simply to observe it. Because they have an abiding impulse to make a difference, to do the right thing and to do it right. Because amid all the noise and nonsense, amid the stresses and strains, amid the revulsion they feel for what they encounter online and the compulsion they feel to counter it, amid all that they bear testimony to a Moral Sense.

Iain Lobban
14.vii.15

With thanks to:

- Tony, the GCHQ Historian, for generously sharing his perspectives from history and ethics;

- Lieutenant General (retired) Sir Graeme Lamb KBE, CMG, DSO for bringing to life for me both the concept and practice of 'Mission Command'; and

- The fellowship of Pembroke College, Cambridge for affording me the status of Visiting Scholar and the inspiring environment in which to draft this lecture.