It has been a fascinating two days. We have debated just what the nature and role of Intelligence Services should be in the years ahead, including any structural changes that may be required for them to provide the most effective support to national and collective security. We started our conference with the perspective of Lord Robertson, the statesman who was Secretary General of NATO on 9/11 and in the crucial years afterwards oversaw the reorientation of NATO towards its new missions. He spoke of the pressing needs of the highest levels of political decision taking, including of those leading international organisations, for reliable intelligence on which to base their policies and response to events. He also reminded us that the past record of our intelligence communities in countering surprise by providing advance notice of aggression has always been patchy. We reflected with him on the huge shift that has taken place in intelligence activity since 9/11 focusing on transnational and non-state actors, insurgents, terrorists, cyber criminals and serious international criminal gangs.

We have also spent much time over the last two days analyzing how best to build and strengthen the necessary international partnerships to support the intelligence mission. These partnerships also have to include those with the private sector, not least in the cyber domain where the cutting edge is often to be found in commercial applications of modern techniques of internet monitoring, data mining, data scraping, data fusion, social media analytics etc. No longer is the future set of technologies for intelligence just a matter for government laboratories and agencies. And inevitably therefore contractors will play a greater part in the work of intelligence communities. But I would enter a caveat here. Public support for the necessary work of intelligence agencies is essential. And certainly in the UK, the public expects the powers of the State to engage in
activities that intrude on the privacy of the citizen to be directed by public servants whose loyalty is to the State and to the public interest and not the profitability of the enterprise.

**Beyond the Intelligence Cycle**¹

I certainly took away from the last few days insights into post-Cold War changes that have been taking place in a number of countries in the way Intelligence Services are organized as a result of the transformations in the nature of foreign and domestic threats we are witnessing. At the same time we were reminded – if any reminder was needed – that though terrorism as an issue has clearly grown in importance, more traditional state-based concerns -such as pre-occupy us with Iran, North Korea, China, and the Middle East – nonetheless remain crucial. In the words of our chair Mark Lowenthal, one agenda has not replaced the other – the total agenda has become longer and more complex, and I might add more technical. The stakes are as high as ever and, as I shall hope to demonstrate, the role of intelligence is even more important than it was. I did wonder therefore whether the title of this conference – The Changing Role of Intelligence – deserved a question mark.

To put the point a different way, do the issues we have discussed add up to the need to rethink what in a democratic society we mean when we talk about intelligence communities and what they do? Is there a need for a new model of intelligence? Let me offer you at the conclusion of this conference one way of trying to think about such questions.

A good place to start is to ask ourselves, what do we teach the newcomers to the profession about their own profession? Indeed, do we teach them to think of intelligence work as a profession? What do we teach customers for intelligence about the processes that produce intelligence? What do we tell suppliers about what the intelligence world is about? The hallmarks of professions are that they

have entry requirements, shared common ethical codes of conduct and discipline, regulation and oversight. The picture here across our nations' intelligence communities is patchy. But we might agree that intelligence analysis – now widely practiced in the private sector of course as well as by government agencies – has every right now to be regarded as a professional skill like statistics with its own accepted methodologies, case studies, best practice and professional ethical codes?

Intelligence teaching often starts (and sometimes ends) with the conventional diagram of the intelligence cycle showing the functions of direction, collection, processing, analysis and assessment and dissemination of product to customers. When I used Google Images I came up with over a hundred examples, not just the CIA, FBI and DIA (each of whose diagrams of the cycle are subtly different) but examples ranging from the Kenyan National Security Intelligence Service to the Iowa Department of Public Safety and with examples from many private sector intelligence and business strategy departments. I am reminded of de Gaulle's remark about the difficulty of governing a nation that produces over 240 different varieties of cheese!

I suggest that the classic intelligence cycle as a model of the totality of today's intelligence activity – let alone tomorrow's - rests on three shaky pillars, each one of which has been implicitly subject to challenge by participants in this conference.

The first concept underlying the cycle is that there is a single agreed intelligence narrative: sequencing functional activities to link the steps said to be involved in producing intelligence, starting with collection of raw secret material from agents, signals interception, imaging satellites and so on, and leading after processing (validation, collation, analysis and assessment) to some form of intelligence reporting to an end user, be they policy maker, military commander or law enforcement officer.

That narrative had intuitive Cold War public appeal. I recently watched again the Kevin Costner film *13 Days in May* when at the heart of the Cuban missile crisis photo-recce sorties are ordered over the island (no doubt leaving cinema...
audiences on the edge of their seats over the danger to the pilots), the resulting raw imagery is processed (with audience tension building over the wait), and interpreted by expert analysts (with the will-they, won’t-they spot the Soviet missiles moment), and the resulting intelligence assessment of the state of preparedness of the Soviet missile deployments delivered by the Director of Central Intelligence in person to a tense National Security Council to help the President decide how much time he has to avert war before the missiles become operational (satisfyingly demonstrating the positive power of intelligence to shape events).

The modern practitioner, however, may well face a rather different public narrative of what intelligence is thought to be about today. The controversy over assessments on Iraqi WMD will no doubt feature (as Lord Robertson reminded us) as well as media reporting of extraordinary rendition, coercive interrogation, internet surveillance and drone strikes. In short, we are in need of a new intelligence narrative that links the important value of intelligence in keeping the public safe with public agreement on where the limits on intelligence activity should properly be set.

Another challenge to the narrative comes from recent technical developments, especially in support of military counter-insurgency and counter-terrorist operations, that place the user at the centre of the cycle and reduce the need for steps in the cycle to be followed strictly sequentially. Modern communications allow fast interaction: targets geo-located by SIGINT or other intelligence and identified as hostile by intelligence analysts can have their coordinates uploaded onto precision guided missiles already airborne carried by drones or combat aircraft in orbit. Valuable intelligence can now come from accessing and mining digital data in government and commercial databases with examples ranging from passport and immigration records to mobile telephone records, airline bookings to financial transaction as well as many other examples. Such data can be exploited to reveal clues to the identities, location, movements, finance and
associations of suspects. Intelligence exploitation of (data protected) personal
data, for which I have coined the term PROTINT makes the intelligence officer
more akin to a detective than the classic intelligence analyst analyzing the
characteristics of the strategic weapons systems of potential adversaries. Most
recently, the explosive growth in social media use on the internet has begun to
provide another source of intelligence, for which the term SOCMINT seems
appropriate. I now usually refer to intelligence access, rather than intelligence
collection, to reflect the existence of these four pools of information: the classic
secret ‘INTs (HUMINT, SIGINT, IMINT, MASINT etc); the huge new domain of
open source intelligence (OSINT); protected personal data (PROTINT); and
finally social media intelligence (SOCMINT).

The steps in the intelligence cycle have never mapped neatly onto the
responsibilities of individual agencies. The exact form of the cycle if shown in
detail would look different, for example, in imagery, signals intelligence and
human intelligence. The now extensive links with overseas liaison services, as
well as differing national organizational structures, also mean that the standard
cycle is unlikely to capture precisely any given nation’s intelligence production
processes. It may well be too that the standard cycle reflects the Anglo-Saxon
cultural prejudices of its originators and that in China or India, for example, their
different philosophical traditions would lead them to a different model.

Given modern cyber developments, it is harder than in the past to construct a
comparably simple narrative for modern intelligence work. Of course,
conventional inter-State intelligence can be assumed to continue, but after 9/11
the emphasis has been on intelligence on non-State actors for immediate action,
whether to protect deployed military forces or identify and locate terrorists, as
well as other current priorities to interdict embargo breaking or proliferation
activities, interrupt narcotics supply or to trigger other forms of operational
military, police or border security activity. The key relationships over the last
decade have been as much those between analysts and military commanders as
policymakers, and increasingly and notably with law enforcement officers.

Intelligence is, however, not evidence, and given the inherent need for maintaining secrecy over sources and methods there will always be limitations on – and controversy over - how far intelligence can be converted into admissible evidence in a proper court of law. To repeat, the intelligence narrative has in the public mind become clouded by questions over the use of intelligence and the methods used to obtain intelligence by our own and liaison services, both from the point of view of allegations of violations of individual rights through coercive interrogation and ill-treatment of suspects and by violation of privacy rights through potentially invasive methods of surveillance and investigation. Our publics clearly are prepared to place a high value on their own security, but as yet lack a consensus on what should be the limits on intelligence work to deliver it, an issue with which Parliamentary and other independent oversight bodies of intelligence communities will have to wrestle in the years to come.

**The interaction with the user and professional intelligence identity**

The second concept underlying the intelligence cycle is that of professional intelligence identity: the separation of the identity of the intelligence professionals from that of their various user communities, especially the policy makers. The cycle shows intelligence being disseminated by producers to the consumers of intelligence (be they end users or analysts in other parts of one’s own or liaison intelligence communities) who then provide feedback on the value of the product in order to refine collection strategies. It is this idea of intelligence having an added value in public policy terms expressed in user response that curls the linear intelligence narrative back on itself in a feedback loop or cycle.

But modern digital communications also enable intelligence products to be available on demand, changing the relationship between the intelligence analyst and the military staff or policy customer. Web-pages and databases of intelligence product (written reports, indexes, watch lists, multi-spectral images, annotated digitized mapping, equipment schematics and the like) can be searched securely on-line and then downloaded as required by the user. This
‘pull’ complements the traditional intelligence cycle’s direction of ‘push’ of product and is a major conceptual development beyond the classic cycle in understanding how modern intelligence works. Both are of course needed and it would be dangerous to rely only on the user pulling data that they already know they want. Winston Churchill’s words on the weaknesses that led to the fall of Singapore are apt: I should have known; I should have been told; but above all I should have asked.

Most versions of the cycle therefore add numerous short-circuits and feedback loops, emphasizing that intelligence flows are not linear and that there are direct interactions between the policymakers and the tasking process over specific requirements such as an approaching Ministerial visit or an international negotiation. There are also many operational connections to refine search parameters or provide names of individuals of intelligence interest for border security and law enforcement. Nor can any simple version of the cycle render visually the cumulative value of assessed intelligence. The assembled whole can reveal far more than the reading of individual intelligence reports that are by their nature usually fragmentary and incomplete.

As Lord Robertson reminded us, the 2002/03 Iraq experience re-ignited old debates within intelligence communities about the importance of intelligence assessments (such as NIE and those from the UK JIC) being regarded as professional advice on a par with professional military or medical advice. Governments need not act on such advice, but have to be accept it for what it is and not cherry pick from it to fit policy. The danger of politicisation of intelligence reporting if analysts and their customers get too comfortable in their relationship has been a concern since the early days of Sherman Kent in the CIA, but the practitioner knows that real life requires a balanced relationship that is neither too close nor too distant. In the words of a distinguished former chair of the JIC, Sir Percy Cradock: “The best arrangement is intelligence and policy in separate but adjoining rooms, with communicating doors and thin partition walls, as in cheap hotels”
The reach of the model of intelligence

The third (meta-)concept underlying the intelligence cycle is that it is indeed possible sensibly to model intelligence activity, specifically by capturing in a cyclical model the specific functional activities that reveal the essence of what intelligence activity is all about. The reach of the model is governed by the choice of which activities to include in the cycle. That choice is, of course, equally a choice to exclude others and to define ‘intelligence’ accordingly, a point of some importance for the practitioner in terms of the boundaries, organization and development of the intelligence community of the future.

What the classic intelligence cycle based on a narrow definition of intelligence activity leaves out is a significant part of the activity of what the members of intelligence agencies actually do, including counter-intelligence and security intelligence. Examples of leveraging secret intelligence to disrupt hostile activities abound, and include the use of deception and sting operations, by intercepting illegal arms shipments and by arresting those involved in terrorist, proliferation or criminal networks. External intelligence services can therefore double as external action services, increasingly with support from Special Forces units within defence. Policy makers increasingly want not just more information bearing on their decisions, they want to know what can be done to achieve their goals by utilising the more intimate knowledge Western intelligence officers may have of the personalities and politics of the leadership of a country of interest, or of opposition groups, than may be possible through conventional diplomatic channels and what opportunities there may be for using agents of influence. In cyberspace too the demand will not just be for information about attacks and recovery but what can be done to neutralise threats themselves. There will be equities to be balanced between the interests of intelligence gathering, of law enforcement and of the protection of national infrastructure. Operating at cyber speed will be of the essence in using such intelligence, for which the classic
intelligence cycle is an inadequate model nor does it illustrate the inherent conflict between gathering intelligence which requires acting as unobtrusively as possible and direct action that can result in very visible results.

Conclusions for the Practitioner

From having been in earlier centuries the covert exercise of the Sovereign’s prerogative powers in defence of the realm, intelligence as described in the UK National Security Strategy\(^3\) has now become an avowed, statutory component of modern government, in domestic as well as in foreign affairs, in law enforcement as much as in statecraft or military operations. With an historical perspective, we can see an underlying three-fold logic to this fundamental shift, even if at the time those involved may well have felt themselves simply responding to the pressure of events, not least from media revelations and human rights pressures.

The starting point was an increasing awareness, as the Cold War came to an end, of a variety of threats to human security, displacing the earlier dominating pre-occupation with the security of the State from Soviet aggression and subversion of democratic institutions. National security now begins to be seen as a state of confidence that the response to the major risks facing the citizen - both malign threats such as terrorism and cyber attacks and natural hazards such as pandemics - is being managed to allow normal life to continue, with markets stable and investment being encouraged.

Accepting that the goal of national security, as seen from the point of view of the citizen, is thus about a sufficient level of protection from all major risks (both threats and hazards) a second step in constructing modern national security policy is to apply the tools of risk management. Here the magnitude of the risk to

be managed can be assessed as the product of several factors that are capable of being influenced by government: the likelihood of the disruptive risk arising; the degree of vulnerability of the nation and its inhabitants to the danger; and the initial impact and duration of danger and disruption should the risk crystallise.

Taking a human view of overall national security thus leads naturally to an increased demand for intelligence to support risk analysis. This has happened in the post-9/11 expansion of intelligence and law enforcement capabilities to detect terrorist networks and frustrate impending plots. But intelligence is also needed to help understand the ideology of the terrorists and explain their motivations and thus help focus work to prevent radicalization and enhance community cohesion. Different types of intelligence must in addition be brought to bear to support investment in protective security, based on deep technical analysis of terrorist capabilities and future intentions.

Here we see a broader ‘intelligence’ function not captured in the classic intelligence cycle: to provide government with strategic notice of possible emerging risks (and opportunities). The intelligence analysts have an important contribution to make to generating strategic notice of possible future threats, and thus avoid strategic surprise, but so do the scientists and technologists with their horizon scanning, the geologists looking at oil and mineral resources, the climatologists modeling future climate change and water stress, the astronomers looking for coronal mass ejections and stray asteroids and the social scientists and anthropologists studying the growth of hostile ideologies and the problems of rapidly increasing global urbanization (in 1800 only one city, Beijing, had a population of 1 million; today there are 381 such conurbations). Where in government does a National Security Council look for consolidated assessment of short- and long-term risks, covering both threats and hazards and using open source and traditional secret sources? To be useful clearly such work has to be fundamentally inter-disciplinary, and to break out of the stockade of secrecy around most intelligence cycle activity.
There are of course limits to the reliance that can be placed on intelligence warning about unexpected threats and hazards. There will always be surprises: the most significant example over the last few years of failure of strategic notice and consequent risk blindness has been the global financial crisis, a threat that did not figure on the risk registers of the UK or other nations. Nevertheless, modern national security policy provides a strong rationale for greater investment in national intelligence capability. There is perhaps a further reason, evident to the policy makers, even if given less stress in public. Over the next decade financial austerity resulting from the need to overcome successive global economic and financial crises will mean reduced levels of expenditure on both hard and soft power capabilities and reductions in the numbers available for domestic law enforcement. Thinking smarter will have to given priority.

One result of the need to do more with less is the harnessing of technical developments in managing and moving data efficiently within intelligence agencies as the sponsors of this conference have amply demonstrated. Now the search is for ways better to integrate and fuse all elements of the process. Intelligence agencies are now knowledge management industries coming to terms with the cultural and structural transformations of the postmodern world.

Over the years, different models have been found useful for thinking about a variety of intelligence problems. For example, we were all taught the distinction between intelligence on a potential adversary’s capabilities and on his intentions. Similarly, many of us will have found useful in analyzing the uncertainties in intelligence estimates to consider that judgments that are about secrets and those that are about mysteries. With such thinking in mind I prefer to think of a model of future intelligence analysis (using intelligence in its broadest sense) to support national security decision making as best thought of
as consisting of four levels of reasoning⁴. Each level has its own analytical methods, and each level attract different kinds of uncertainties in making key judgments.

The first level is that of situational awareness. The primary use of intelligence, and by far the greatest in terms of volume of effort involved, will continue to be what I term building situational awareness, to answer questions of ‘what, where, who?’ Intelligence reporting is always fragmentary, incomplete and must be assumed even after validations sometimes to turn out to be just wrong. But used systematically, over a period government and its various organs will be in a position to take better decisions than simply relying on hearsay or political whim. In the military domain especially, great strides have been made in providing reliable situational awareness through fusing the inputs from a variety of sensors

A second essential dimension in using intelligence in supporting decision-making is, however, in building an explanatory theory of past and present behaviour, answering the questions ‘why and what for?’ Such explanatory theories are important in understanding, and more importantly not misunderstanding, the behaviour of foreign states, for example, whether military deployments should be taken as indicators of defensive or offensive intent of nations, and of the motives of non-state groups such as insurgents or terrorists.

Good intelligence assessment thus has explanatory value in helping deepen real understanding of how a situation has arisen, the dynamics between the parties and what the motivations of the actors involved are - as they, not we, see them – and thus how they might be perceiving our side’s moves. Providing such satisfactory explanation requires a detailed knowledge of the country concerned,

the languages, personalities, local cultures, history, commerce and topography. Developing expert analysts capable of such deep understanding represents a major challenge for all intelligence communities. What is required at this level of thinking about security is deep understanding of the phenomena in question, and their roots and causes and possible future development, expressed in ways that will help the military or policy staffs develop options for decision makers. Working effectively at this level is hard: are we really any better served in that respect today?

Having a satisfactory explanation of events is a necessary precondition to producing well-founded predictive assessments since the third level of intelligence judgment is prediction, answering the questions ‘what next?’ or ‘where next?’. It could be fundamental to grand strategy, such as estimates of the likelihood of conflict over oil exploration in the South Atlantic or South China Sea, or of tactical significance such as identification of the intended target of a terrorist attack. It could be a predictive assessment based not on specific intelligence reporting but on judgments made about a developing situation that extends the explanatory into the predictive. In the case of failure to predict revolutionary change what is likely to matter is the ‘feel’ that the analyst has for the interactive dynamics of the developing situation rather than any specific secret intelligence.

Intelligence prediction beyond a short time ahead is next to impossible. A fourth, separate, category is needed in this model of modern intelligence to support national security planning and that is ‘strategic notice’ of possible future risk-related developments especially where these might invalidate the explanations and predictions being made by the analysts in their risk matrices. These are possible futures worthy of attention, but not predictions that they will necessarily come about. One of the most important benefits of good strategic notice is in enhancing the ability of government to commission full intelligence assessments or longer-term scientific and other research to illuminate the
phenomena, which should be done systematically as a cross-government exercise. Open sources come into their own here and intelligence organisations will have to be strategic, engaging more with outside experts, and developing a more rigorous intelligence community training program. Several nations represented here have already taken steps to develop a stronger 'strategic notice' capability.

There is at the heart of intelligence work, a simple truth. The most basic purpose of intelligence today remains the same as it was centuries ago, to help improve the quality of decision making by reducing ignorance. The nature of those decisions has changed over time, and today is governed by the demands of national security strategy for information to help manage a wide range of major risks. The speed of technological change challenges our ability to adapt with the pervasiveness of the technology reaching into every aspect of our lives – and thus providing new opportunities for intelligence gathering. And that increase in potential supply is coinciding with an increase in demand for real time intelligence on so-called non-state actors, terrorists and the like.

As already noted, the purpose of the secret component of intelligence is simply to improve decision taking with information that other people do not want you to have, from which flow all of the characteristic moral hazards associated with the world of intelligence so beloved of fiction.

A final reflection: secret intelligence cannot be obtained without using techniques that overcome the will of the person with the secrets who is determined to keep them secret. The ethical implications of that inconvenient fact could be ignored by most governments running intelligence operations during the 20th century; intelligence in the 21st century is, however, no longer an ethics-free zone and the democratic acceptability of its methods may well end up
shaping more of the future role of intelligence than developments in technology, amazing though those will no doubt be.