Contents

Preface to the paperback edition

So much has happened in less than a year since this book was first published in autumn 2020 that the least I owe the reader is an updating preface to introduce the paperback edition. Time seems to have speeded up for world events, while slowing down for those of us shielding for the last year from the COVID-19 pandemic and watching, as if in slow motion, a series of extraordinary events unfold. It is no comfort to me that all the themes in this book have been illustrated in primary colours over that short period.

I started writing this book after seeing how the Brexit referendum and the 2016 US Presidential election were being reflected on social media. What I was horrified to see was a rising tide of half-truths and distortions designed to try to persuade us online of what we ought to think and want. Not to mention seeing some downright falsehoods and deceptions, coming not only from Russia, aimed at creating a hostile atmosphere, widening divisions in our societies and increasingly setting us at each other's throats. The failed insurrection of the supporters of President Trump, their storming of Congress and his historic impeachment by Congress for the second time have illustrated one of the key lessons of the book – the power of social media to mobilize the energy of individuals for causes, good or ill. The failure of that attempt to overturn the legitimate outcome of the US election does nevertheless give me confidence that I am justified in ending the book on a note

of optimism over the strength of democracy provided we look after it. But it has been a close-run thing in the US.

Ironically, Facebook's founder, Mark Zuckerberg, had changed the company's mission statement the year after the 2016 US election from 'making the world more open and connected' to a more action-oriented appeal to 'give people the power to build community and bring the world closer together'. An admirable sentiment but, as so often happens, one that was to be realized in an unforeseen way. The sections of the Republican community that had so passionately supported Donald Trump's election in 2016 used social media to come even closer together, but only to end up violently contesting the 2020 election result on the basis of the President's baseless claim that it was being stolen, a case where social media had induced the transition from 'I would like it to be true' to, with constant repetition, 'It might be true', which, despite proof to the contrary, slid too easily for the Trump base into 'For me, it is as good as true – and I will act believing it to be true.' More than three years after Facebook's change of mission statement, some of those groups have done exactly what Mark Zuckerberg envisioned: they have bound themselves together for a passionately held common cause. But their 'something greater than ourselves' wasn't what Zuckerberg had had in mind: a seditious movement upsetting the peaceful transfer of power following a fair and certified election in the United States. As I explain in the book, we must now recognize that sedition and subversion have gone digital.

Only time will tell whether the social media giants will acknowledge that the problem lies deep in the very architecture of their platforms. They have been built to encourage the personalized advertising technology that pays for the platform, based on identifying groups of users with similar opinions and characteristics from their personal data, including from their

internet usage. A *Wall Street Journal* article from May 2020 reported an alarming finding from Facebook's own researchers. According to a 2016 internal Facebook study, '64 percent of all extremist group joins are due to our recommendation tools . . . Our recommendation systems grow the problem.' One user found that the more he posted deranged Trumpist messages, the more followers Facebook sent his way, and soon he was effectively hosting a group based on election denial, with tens of thousands of members. Thereby hangs the myth of 'the steal' of the Presidency by Joe Biden – a conspiracy still believed by millions of heavily armed US voters. That story has not ended.

I remind us in the book why so much online content works at an emotional not a rational level. It is a toxic combination when the inherent characteristics of the business model of the Internet combine with our human psychological vulnerability when online. We are targeted with the political messages that the algorithms have revealed are most likely to trigger our emotional response, just as we are targeted by marketing for specific products and services that the algorithms have concluded we ought to have an interest in – without our realizing how we are being manipulated. I was struck recently by the words of Jimmy Wales, co-creator of Wikipedia: 'If you think about advertising-driven social media, the real incentive is to show you as many ads as possible . . . and it's driven them to create addictive products. It's driven them, in many cases, to prioritize agitation and argumentation, in a negative sense, over education and learning and thoughtfulness.'

It is worth re-emphasizing that the Internet is a marvellous, life-enhancing invention. We are dependent on the Internet for our future economic and social development. It is as well that the COVID-19 pandemic did not strike us twenty years ago

when we would not have had the apps that have helped us to video call loved ones, to work from home, to provide online education and to allow us to purchase food and goods online. We have nevertheless been forcibly reminded that the Internet has a dark side. Twitter finally banished President Trump from its platform after he appeared to have incited the mob to march on Congress, and that appears to have led to a marked decline in offensive tweets, although there is some evidence that these have moved to other niche platforms used by the far right. It is a good sign that Facebook is stepping up its content moderation and agreeing to be bound by the decisions reached by an independent oversight board of lawyers, journalists, human rights advocates and other academics. Those who wield power in cyberspace have to accept their heavy social responsibility.

As I describe in the book, social media allows the micro-targeting of political messages tailored to the feelings of different audiences having, as we have seen, a transformational impact on traditional politics. I am not naive about the old practice of politics. You cannot be a Permanent Secretary of a major department of state in Whitehall without understanding the sometimes brutal realities of the democratic process. Social media provides a powerful persuasive tool and as such will be used in the contest that is the competition for power. The sensible public has always understood that traditional political debate has its political swagger and exaggeration. And we have always known that personal ambitions and bitter political rivalries are inseparable from the contest that is democratic politics. But we should not have to suffer those who blur, or even deny, the very nature of truth. No one is entitled to their own alternative facts, and I have been gratified by the way that readers of the earlier edition of this book have responded to endorse that message.

Another internet concern tackled in the book through the lens of intelligence is the prevalence of conspiracy stories spread by social media. Recent months have seen telling examples swirling around COVID-19 and drawing in long-term anti-vaxxers, with potentially disastrous consequences for those who act on these conspiratorial ideas, and causing harm for all of us. We have had unfounded claims that the vaccines will cause mutations in the RNA sequence of those who take it. And of government ambitions to control the lives of citizens through forced vaccinations, alleging that those who do not take the vaccine will lose their jobs and their children be barred from school, or even that they will be kept from going out in public. We have had fantasist stories both that COVID-19 is a hoax and that it is a US bioweapon gone rogue. There has been a media campaign in Russia falsely denigrating the Oxford University / AstraZeneca vaccine as being dangerous to humans (labelling it 'the monkey vaccine'). We still see Russian media trying to erode Western public confidence by highlighting the few recorded cases of side effects from the approved vaccines. Then last year we had the home-grown conspiracy story spread on social media that emissions from 5G mobile-phone masts can cause COVID-19, leading to attacks on mobile-phone masts in some major cities in England. That baseless claim capitalized on years of conspiracy beliefs that mobile phones cause a range of medical harms. Combating falsehoods that mislead the public on the facts about disease and health measures has become an important role for public health. Again, the gravity of the pandemic and the reputational damage the social media platforms are suffering have triggered them into adding warnings to posts about the disease from their platforms, removing the most dangerous of them and de-platforming the worst offenders.

I have been much encouraged by the many comments posted by those who have read the book and who have found it helpful to use my model of analysis to help them understand the experience of COVID-19. A good example comes from the anticipated emergence of different natural mutations of the virus as it infected more and more people. We must be grateful for the past investment in UK bioscience that provided the capability to gene-sequence viral samples from many patients. Therefore, the scientists in the UK were quick to detect signs of increasing numbers of people infected with a particular new variant in Kent and spreading elsewhere. In the language of my model, they had *situational awareness* to answer questions about the 'what and where' of events. Then came the essential step of providing scientific *explanation* of what was being observed, in terms of a mutation on that part of the virus called the spike protein, giving the variant a selective advantage and making the virus more transmissible. With sufficient data and that sound explanation, the modellers were then able to provide ministers with useable *estimates* of likely increased transmissibility and to apply that modelling to the likely consequential increase in the R number over time. It matters, of course, in the modellers' forecasts what they have assumed about future public compliance with lockdown or the transmissibility of a new variant. Disagreements between professionals often boil down to disagreement about the appropriateness of assumptions to use in the model. I describe in the book how that same analytic progression is used by intelligence analysts assembling the basis for warning assessments for the National Security Council – for example, of signs of hostile activity around the world in cyberspace or that could affect our interests and the safety of the public.

But I warn in the book that while we are so closely focused on examining current threats we may find an unwelcome and unexpected surprise comes and hits us on the back of the head. So let me emphasize here the value of what I term *strategic notice* of possible future developments of concern. Strategic notice helps contingency planning, answering important questions of the 'How could we best prepare for whatever might appear next?' type, or even 'How could we pre-empt this risk so that it never comes to test us?'

With strategic notice we may be able to mitigate the risk: for example, by commissioning relevant research or investing in greater resilience. To develop the COVID-19 example, we had plenty of strategic notice of a new coronavirus pandemic (it was top of the risk matrix in my time as UK Security and Intelligence Coordinator, although we assessed it was most likely to be in the form of a mutated flu virus). The good news is that there was then significant investment in the research capability to develop and test vaccines much faster than ever before. We see the beneficial results today. The bad news was that despite the strategic notice there was not the investment in related resilience, so when this particular pandemic arrived, the UK did not have stocks of protective clothing and masks even to cover the immediate needs of health and care-home workers (nor up-to-date plans of how to acquire more, quickly) and did not have rehearsed plans to expand rapidly existing local track-and-trace systems. Another important lesson of intelligence is that by paying heed to strategic notice we do not have to be so surprised by surprise. Taken together, those outputs from rational analysis form the SEES model: situational awareness; explanation; estimation and modelling; and finally strategic notice.

The appearance of new, more dangerous variants of the disease and the increasing heartbreak from its economic ravages

and divisive social and educational effects have led to public questioning of how far politicians have been, as they claim, 'following the science'. The tension between rational analysis and political mandate is another key theme of the book that has been exposed in recent events.

In government, professional analysts and policymakers inhabit largely different domains (in part a deliberate organizational arrangement to reduce the risk of perceptions of political bias creeping into professional assessment). The inhabitants of these domains therefore need to take the trouble to understand each other and how far to expose any remaining disagreements, such as we see reported today in arguments over measures to restrict the spread of COVID-19 disease, such as closing schools. The processes of analysis and its complexities can seem abstract and remote from the people-dominated world of the politician; but analysts too often see policy driven by magical thinking, believing that the announced objective or target will be achieved without assurance that the real-world mechanisms and resources are on the ground capable of securing it. Sometimes there can be specific 'warning failures' that fall into the cracks between adequate foreknowledge and appropriately swift precautionary action: hearing the words but not listening to the message. Misunderstanding can arise because professionals and policymakers have failed sufficiently to probe each other's position. The answer you get from professionals does depend on the precise question you asked. When I was Permanent Secretary in the Home Office, my brilliant chief lawyer, the late Dame Juliet Wheldon, used to insist that I not ask her what the law says but to tell her honestly what I needed to achieve so she could then give me her professional judgement as to whether it could be achieved within the law, and if so how. For law, substitute science.

In the book I describe the risks of hostile activity in cyberspace, but I did not imagine that threat would be so dramatically highlighted by Russia being caught recently conducting one of largest cyber-espionage campaigns ever (codename SolarWinds) against the United States. I warn in the book that subversion and sedition have now gone digital. I was not surprised that the Russian intelligence agencies would try to silence and discredit President Putin's principal domestic critic, Alexei Navalny. But I confess to being taken aback that they would resort to old-fashioned murder to remove him and that, even after the exposure of their bungled attempt to murder Sergei Skripal and his daughter in Salisbury in 2018, they would choose to do this by using the illegal nerve agent Novichok, bringing even more international condemnation on their heads. I was not surprised, however, that it was the open-source intelligence group Bellingcat, working with investigative journalists, that was able to pin this on the FSB, Russia's domestic-security agency. Clever intelligence gathering and analysis in the digital age are not confined to secret agencies.

I must thank all those who have read the book and fed back to me their wide experience of decisionmaking under uncertainty. The CEO of a major British FTSE company told me he had read the book and it had already changed the way he thought about pending decisions on major contracts and customer relationships. He sent copies of the book to all his senior managers with the injunction to use the SEES model, and to apply its lessons to negotiation and forming lasting partnerships based on demonstrating a record of trustworthiness. Likewise, the MD of a cybersecurity company has told me he has sent copies of the book to all his contacts with a similar message. I am glad of this direct evidence that the SEES model

is being of practical use in answering the question of what we need to know to take solid evidence-based decisions.

I have kept the description of the SEES model as it was in the first edition. But I was struck by the comments of one correspondent who felt I could have been clearer that, in arguing for more rationality in the taking of decisions, I was not trying to banish the feelings which drive big decisions and motivate genuine political engagement. I am happy to use this preface to reassure on that point and to expand on my thinking. I do not wish to be read as being secretly tempted to want government handed over to the modern equivalent of Plato's unelected guardians. The cost–benefit analyst does not always know best. Understanding well what is, does not tell us what we ought to strive for.

It is the same when it comes to making a big personal decision. We have to bring together in our own head two different qualities of thought: on the one hand, rational analysis of the situation we are in and the options open; and, on the other hand, understanding what our ambitions are for what we want to achieve by our choice, or what outcomes we fear and wish to avoid and what our values tell us we should do. Both kinds of thought, the dispassionate and the impassioned, the 'what is' and the values-driven 'what we hope will be', need to be understood and integrated if we are to make sound decisions. However imperfectly, it is what I have tried to do myself facing difficult choices. One personal example was deciding to seek another senior post after only just surviving treatment for the life-threatening cancer that had forced me to stand down in 2001 as Permanent Secretary to the Home Office. I had to balance the professional medical advice I had been given of the continuing risks with a sense of continuing duty and, I confess, a residual ambition to make a difference. I ended up accepting

the Prime Minister's offer that I become the first UK Security and Intelligence Coordinator in the Cabinet Office, a tough assignment but one that I have never regretted taking.

Much of the problem I describe with the use of social media today is that it reduces the analytic input in favour of the emotional. On social media we can feel our emotional responses being heightened. The motivations (including aspects that were previously unconscious to us) that lead us to feel we want to make a decision surface more vividly into our mind. At the level of advertising, for example, we experience too readily mimetic desire, wanting what other people want (or social media influencers induce us to want). We all can suffer too in our thinking from the cognitive biases that I describe in Chapter 5. We may, for example, have been selective about the facts we chose to emphasize as important, or we may have been attracted by explanations of events with which we felt most comfortable and ignored those that ran counter to our instincts. It can be a dangerous combination when we undervalue the use of rational analysis and when we do not realize that the analysis itself is less objective than we believe it to be.

Bringing these types of thinking, rational analysis and personal desires, together inside a single mind has always been hard. I hope that this book will encourage readers to find ways of using the method I describe to arrive at results for their own decisions that feel right to them but are grounded firmly in reality. But a warning message that the book offers is to take extra care to check that rational analysis has its proper place. Achieving that is getting harder now we are in the digital age of social media.

David Omand
February 2021

Introduction

Why we need these lessons in seeking independence of mind, honesty and integrity

Westminster, March 1982. 'This is very serious, isn't it?' said Margaret Thatcher. She frowned and looked up from the intelligence reports I had handed her. 'Yes, Prime Minister,' I replied, 'this intelligence can only be read one way: the Argentine Junta are in the final stages of preparing to invade the Falkland Islands, very likely this coming Saturday.'

It was the afternoon of Wednesday, 31 March 1982.

I was the Principal Private Secretary to the Defence Secretary, John Nott. We were in his room in the House of Commons drafting a speech when an officer from the Defence Intelligence Staff rushed down Whitehall with a locked pouch containing several distinctive folders. I knew immediately from the red diagonal crosses on their dark covers that they contained top secret material with its own special codeword (UMBRA), denoting that they came from the Government Communications Headquarters (GCHQ).

The folders contained decrypted intercepts of Argentine naval communications. The messages showed that an Argentine submarine had been deployed on covert reconnaissance around the Falklands capital, Port Stanley, and that the Argentine Fleet, which had been on exercises, was reassembling. A further intercept referred to a task force said to be due to arrive at an unstated destination in the early hours of Friday, 2 April. From their analysis of the coordinates of the naval vessels, GCHQ had concluded that its destination could only be Port Stanley.[1]

John Nott and I looked at each other with but one thought, loss of the Falkland Islands would bring a major existential crisis for the government of Margaret Thatcher: the Prime Minister must be told at once. We hurried down the Commons corridor to her room and burst in on her.

The last assessment she had received from the UK Joint Intelligence Committee (JIC) had told her that Argentina did not want to use force to secure its claim to the sovereignty of the Falkland Islands. However, the JIC had warned that if there was highly provocative action by the British towards Argentine nationals, who had landed illegally on the British South Atlantic island of South Georgia, then the Junta might use this as a pretext for action. Since the UK had no intention of provoking the Junta, the assessment was wrongly interpreted in Whitehall as reassuring. That made the fresh intelligence reports all the more dramatic. It was the first indication that the Argentine Junta was ready to use force to impose its claim.

The importance for us of being able to reason

The shock of seeing the nation suddenly pitched into the Falklands crisis is still deeply etched in my memory. It demonstrated to me the impact that errors in thinking can have. This is as true for all life as it is for national statecraft. My objective in writing this book therefore is an ambitious one: I want to empower people to make better decisions by learning how intelligence analysts think. I will provide lessons from our past to show how we can know more, explain more and anticipate more about what we face in the extraordinary age we now live in.

There are important life lessons in seeing how intelligence analysts reason. By learning what intelligence analysts do when they tackle problems, by observing them in real cases from recent history, we will learn how they order their thoughts and how they distinguish the likely from the unlikely and thus make better judgements. We will learn how to test alternative explanations methodically and judge how far we need to change our minds as new information arrives. Sound thinkers try to understand how their unconscious feelings as individuals, as members of a group and within an institution might affect their judgement. We will also see how we can fall victim to conspiracy thinking and how we can be taken in by deliberate deception.

We all face decisions and choices, at home, at work, at play. Today we have less and less time to make up our minds than ever before. We are in the digital age, bombarded with contradictory, false and confusing information from more sources than ever. Information is all around us and we feel compelled to respond at its speed. There are influential forces at play ranged against us pushing specific messages and opinions through social media. Overwhelmed by all this information, are we less, or more, ignorant than in previous times? Today more than ever, we need those lessons from the past.

Looking over the shoulder of an intelligence analyst

Over the centuries, generals naturally learned the advantage that intelligence can bring. Governments today deliberately equip themselves with specialist agencies to access and analyse information that can help them make better decisions.[2] Britain's Secret Intelligence Service (MI6) runs human agents

overseas. The Security Service (MI5) and its law enforcement partners investigate domestic threats and conduct surveillance on suspects. The Government Communications Headquarters (GCHQ) intercepts communications and gathers digital intelligence. The armed forces conduct their share of intelligence gathering in their operations overseas (including photographic intelligence from satellites and drones). It is the job of the intelligence analyst to fit all the resulting pieces together. They then produce assessments that aim to reduce the ignorance of the decisionmakers. They find out what is happening, they explain why it is happening and they outline how things might develop.[3]

The more we understand about the decisions we have to take, the less likely it is that we will duck them, make bad choices or be seriously surprised. Much of what we need can come from sources that are open to anyone, provided sufficient care is taken to apply critical reasoning to them.

Reducing the ignorance of the decisionmaker does not necessarily mean simplifying. Often the intelligence assessment has to warn that the situation is more complicated than they had previously thought, that the motives of an adversary are to be feared and that a situation may develop in a bad way. But it is better to know than not. Harbouring illusions on such matters leads to poor, or even disastrous, decisions. The task of the intelligence officer is *to tell it as it is* to government. When you make decisions, it is up to you to do the same to yourself.

The work of intelligence officers involves stealing the secrets of the dictators, terrorists and criminals who mean us harm. This is done using human sources or technical means to intrude into the privacy of personal correspondence or conversations. We therefore give our intelligence officers a licence to operate by ethical standards different from those we would hope to see applied in everyday life, justified by the reduction in harm to

the public they can achieve.[4] Authoritarian states may well feel that they can dispense with such considerations and encourage their officers to do whatever they consider necessary, regardless of law or ethics, to achieve the objectives they have been set. For the democracies such behaviours would quickly undermine confidence in both government and intelligence services. Consequently, intelligence work is carefully regulated under domestic law to ensure it remains necessary and proportionate. I should therefore be clear. This book does not teach you how to spy on others, nor should it encourage you to do so. I want, however, to show that there are lessons from the *thinking* behind secret intelligence from which we can all benefit. This book is a guide to thinking straight, not a manual for bad behaviour.

Nor does thinking straight mean emotionless, bloodless calculation. 'Negative capability' was how the poet John Keats described the writer's ability to pursue a vision of artistic beauty even when it led to uncertainty, confusion and intellectual doubt. For analytic thinkers the equivalent ability is tolerating the pain and confusion of not knowing, rather than imposing ready-made or omnipotent certainties on ambiguous situations or emotional challenges. To think clearly we must have a scientific, evidence-based approach which nevertheless holds a space for the 'negative capability' needed to retain an open mind.[5]

Intelligence analysts like to look ahead, but they do not pretend to be soothsayers. There are always going to be surprise outcomes, however hard we try to forecast events. The winner of the Grand National or the Indy 500 cannot be known in advance. Nor does the favourite with the crowds always come out in front. Events sometimes combine in ways that seem destined to confound us. Importantly, risks can also provide

opportunities if we can use intelligence to position ourselves to take advantage of them.

Who am I to say this?

Intelligence agencies prefer to keep quiet about successes so that they can repeat them, but failures can become very public. I have included examples of both, together with a few glimpses from my own experience – one that spans the startling development of the digital world. It is sobering to recall that in my first paid job, in 1965, in the mathematics department of an engineering company in Glasgow, we learned to write machine code for the early computers then available using five-character punched paper tape for the input. Today, the mobile device in my pocket has immediate access to more processing power than there was then in the whole of Europe. This digitization of our lives brings us huge benefits. But it is also fraught with dangers, as we will examine in Chapter 10.

In 1969, fresh out of Cambridge, I joined GCHQ, the British signals intelligence and communications security agency, and learned of their pioneering work applying mathematics and computing to intelligence. I gave up my plans to pursue a doctorate in (very) theoretical economics, and the lure of an offer to become an economic adviser in HM Treasury. I chose instead a career in public service that would take me into the worlds of intelligence, defence, foreign affairs and security. In the Ministry of Defence (MOD), as a policy official, I used intelligence to craft advice for ministers and the Chiefs of Staff. I had three tours in the Private Office of the Secretary of State for Defence (serving six of them, from Lord Carrington in 1973 to John Nott in 1981) and saw the heavy burden of decision-making in crisis that rests at the political level. I saw how

valuable good intelligence can be, and the problems its absence causes. When I was working as the UK Defence Counsellor in NATO Brussels it was clear how intelligence was shaping arms control and foreign policy. And as the Deputy Under Secretary of State for Policy in the MOD I was an avid senior customer for operational intelligence on the crisis in the former Yugoslavia. In that role I became a member of the Joint Intelligence Committee (JIC), the most senior intelligence assessment body in the UK, on which I served for a total of seven years.

When I left the MOD to go back to GCHQ as its Director in the mid-1990s, computing was transforming the ability to process, store and retrieve data at scale. I still recall the engineers reporting triumphantly to me that they had achieved for the first time stable storage of a terabyte of rapidly accessible data memory – a big step then although my small laptop today has half as much again. Even more significantly, the Internet had arrived as an essential working domain for professionals, with the World Wide Web gaining in popularity and Microsoft's new Hotmail service making email a fast and reliable form of communication. We knew digital technology would eventually penetrate into every aspect of our lives and that organizations like GCHQ would have to change radically to cope.[6]

The pace of digital change has been faster than predicted. Then, smartphones had not been invented and nor of course had Facebook, Twitter, YouTube and all the other social media platforms and apps that go with them. What would become Google was at that point a research project at Stanford. Within this small part of my working lifetime, I saw those revolutionary developments, and much more, come to dominate our world. In less than twenty years, our choices in economic, social and cultural life have become dependent on accessing

networked digital technology and learning to live safely with it. There is no way back.

When I was unexpectedly appointed Permanent Secretary of the Home Office in 1997, it brought close contact with MI5 and Scotland Yard. Their use of intelligence was in investigations to identify and disrupt domestic threats, including terrorist and organized crime groups. It was in that period that the Home Office drew up the Human Rights Act and legislation to regulate and oversee investigatory powers to ensure a continual balancing act between our fundamental rights to life and security and the right to privacy for our personal and family life. My career as a Permanent Secretary continued with three years in the Cabinet Office after 9/11 as the first UK Security and Intelligence Coordinator. In that post, rejoining the JIC, I had responsibility for ensuring the health of the British intelligence community and for drawing up the first UK counter-terrorism strategy, CONTEST, still in force in 2020 as I write.

I offer you in this book my choice of lessons drawn from the world of secret intelligence both from the inside and from the perspective of the policymaker as a user of intelligence. I have learned the hard way that intelligence is difficult to come by, and is always fragmentary and incomplete, and is sometimes wrong. But used consistently and with understanding of its limitations, I know it shifts the odds in the nation's favour. The same is true for you.

SEES: a model of analytical thinking

I am now a visiting professor teaching intelligence studies in the War Studies Department at King's College London, at

Sciences Po in Paris and also at the Defence University in Oslo. My experience is that it really helps to have a systematic way of unpacking the process of arriving at judgements and establishing the appropriate level of confidence in them. The model I have developed – let me call it by an acronym that recalls what analysts do as they look at the world, the *SEES* model – leads you through the four types of information that can form an intelligence product, derived from different levels of analysis:

- **Situational awareness** of what is happening and what we face now.
- **Explanation** of why we are seeing what we do and the motivations of those involved.
- **Estimates** and forecasts of how events may unfold under different assumptions.
- **Strategic notice** of future issues that may come to challenge us in the longer term.

There is a powerful logic behind this four-part SEES way of thinking.

Take as an example the investigation of far-right extremist violence. The first step is to find out as accurately as possible what is going on. As a starting point, the police will have had crimes reported to them and will have questioned witnesses and gathered forensic evidence. These days there is also a lot of information available on social media and the Internet, but the credibility of such sources will need careful assessment. Indeed, even well-attested facts are susceptible to multiple interpretations, which can lead to misleading exaggeration or underestimation of the problem.

We need to add meaning so that we can explain what is really going on. We do that in the second stage of SEES by constructing the best explanation consistent with the available

evidence, including an understanding of the motives of those involved. We see this process at work in every criminal court when prosecution and defence barristers offer the jury their alternative versions of the truth. For example, why are the fingerprints of an accused on the fragments of a beer bottle used for a petrol bomb attack? Was it because he threw the bottle, or is the explanation that it was taken out of his recycling box by the mob looking for material to make weapons? The court has to test these narratives and the members of the jury have then to choose the explanation that they think best fits the available evidence. The evidence rarely speaks for itself. In the case of an examination of extremist violence, in the second stage we have to arrive at an understanding of the causes that bring such individuals together. We must learn what factors influence their anger and hatred. That provides the explanatory model that allows us to move on to the third stage of SEES, when we can estimate how the situation may change over time, perhaps following a wave of arrests made by the police and successful convictions of leading extremists. We can estimate how likely it is that arrest and conviction will lead to a reduction in threats of violence and public concern overall. It is this third step that provides the intelligence feedstock for evidence-based policymaking.

The SEES model has an essential fourth component: to provide strategic notice of longer-term developments. Relevant to our example we might want to examine the further growth of extremist movements elsewhere in Europe or the impact on such groups were there to be major changes in patterns of refugee movements as a result of new conflicts or the effects of climate change. That is just one example, but there are very many others where anticipating future developments is essential to allow us to prepare sensibly for the future.

The four-part SEES model can be applied to any situation that concerns us and where we want to understand what has happened and why and what may happen next, from being stressed out at a situation at work to your sports team losing badly. SEES is applicable to any situation where you have information, and want to make a decision on how best to act on it.

We should not be surprised to find patterns in the different kinds of error tending to occur when working on each of the four components of the SEES process. For example:

- Situational awareness suffers from all the difficulties of assessing what is going on. Gaps in information exist and often evoke a reluctance to change our minds in the face of new evidence.
- Explanations suffer from weaknesses in understanding others: their motives, upbringing, culture and background.
- Estimates of how events will unfold can be thrown out by unexpected developments that were not considered in the forecast.
- Strategic developments are often missed due to too narrow a focus and a lack of imagination as to future possibilities.

The four-part SEES approach to assessment is not just applicable to affairs of state. At heart it contains an appeal to rationality in all our thinking. Our choices, even between unpalatable alternatives, will be sounder as a result of adopting systematic ways of reasoning. That includes being able to distinguish between what we know, what we do not know and what we think may be. Such thinking is hard. It demands integrity.

Buddhists teach that there are three poisons that cripple the mind: anger, attachment and ignorance.[7] We have to be

conscious of how emotions such as anger can distort our perception of what is true and what is false. Attachment to old ideas with which we feel comfortable and that reassure us that the world is predictable can blind us to threatening developments. This is what causes us to be badly taken by surprise. But it is ignorance that is the most damaging mental poison. The purpose of intelligence analysis is to reduce such ignorance, thereby improving our capacity to make sensible decisions and better choices in our everyday lives.

On that fateful day in March 1982 Margaret Thatcher had immediately grasped what the intelligence reports were telling her. She understood what the Argentine Junta appeared to be planning and the potential consequences for her premiership. Her next words demonstrated her ability to use that insight: 'I must contact President Reagan at once. Only he can persuade Galtieri [General Leopoldo Galtieri, the Junta's leader] to call off this madness.' I was deputed to ensure that the latest GCHQ intelligence was being shared with the US authorities, including the White House. No. 10 rapidly prepared a personal message from Thatcher to Reagan asking him to speak to Galtieri and to obtain confirmation that he would not authorize any landing, let alone any hostilities, and warning that the UK could not acquiesce in any invasion. But the Argentine Junta stalled requests for a Reagan conversation with Galtieri until it was much too late to call off the invasion.

Only two days later, on 2 April 1982, the Argentine invasion and military occupation of the Islands duly took place. There was only a small detachment of Royal Marines on the Islands and a lightly armed ice patrol ship, HMS *Endurance*, operating in the area. No effective resistance was possible. The Islands were too far away for sea reinforcements to arrive within the two days' notice the intelligence had given us, and the sole

airport had no runway capable of taking long-distance troop-carrying aircraft.

We had lacked adequate situational awareness from intelligence on what the Junta was up to. We had failed to understand the import of what we did know, and therefore had not been able to predict how events would unfold. Furthermore, we had failed over the years to provide strategic notice that this situation was one that might arise, and so had failed to take steps that would have deterred an Argentine invasion. Failures in each of the four stages of SEES analysis.

All lessons to be learned.

How this book is organized

The four chapters in the first part of this book are devoted to the aforementioned SEES model. Chapter 1 covers how we can establish situational awareness and test our sources of information. Chapter 2 deals with causation and explanation, and how the scientific method called Bayesian inference, allows us to use new information to alter our degree of belief in our chosen hypothesis. Chapter 3 explains the process of making estimates and predictions. Chapter 4 describes the advantage that comes from having strategic notice of long-term developments.

There are lessons from these four phases of analysis in how to avoid different kinds of error, failing to see what is in front of us, misunderstanding what we do see, misjudging what is likely to follow and failing to have the imagination to conceive of what the future may bring.

Part Two of this book has three chapters, each drawing out lessons in how to keep our minds clear and check our reasoning.

We will see in Chapter 5 how cognitive biases can subconsciously lead us to the wrong answer (or to fail to be able to answer the question at all). Being forewarned of those very human errors helps us sense when we may be about to make a serious mistake of interpretation.

Chapter 6 introduces us to the dangers of the closed-loop conspiratorial mindset, and how it is that evidence which ought to ring alarm bells can too often be conveniently explained away.

The lesson of Chapter 7 is to beware deliberate deceptions and fakes aimed at manipulating our thinking. There is misinformation, which is false but circulated innocently; malinformation, which is true but is exposed and circulated maliciously; and disinformation, which is false, and that was known to be false when circulated for effect. The ease with which digital text and images can be manipulated today makes these even more serious problems than in the past.

Part Three explores three areas of life that call for the intelligent use of intelligence.

The lessons of Chapter 8 are about negotiating with others, something we all have to do. The examples used come from extraordinary cases of secret intelligence helping to shape perceptions of those with whom governments have to negotiate, and of how intelligence can help build mutual trust – necessary for any arms control or international agreement to survive – and help uncover cheating. We will see how intelligence can assist in unravelling the complex interactions that arise from negotiations and confrontations.

Chapter 9 identifies how you go about establishing and maintaining lasting partnerships. The example here is the successful longstanding '5-eyes' signals intelligence arrangement between the US, the UK, Canada, Australia and New Zealand,