



Contents

[Preface to the paperback edition](#)

[Introduction. Why we need these lessons in seeking independence of mind, honesty and integrity](#)

PART ONE: AN ANALYST SEES: FOUR LESSONS IN ORDERING OUR THOUGHTS

[Lesson 1: Situational awareness. Our knowledge of the world is always fragmentary and incomplete, and is sometimes wrong](#)

[Lesson 2: Explanation. Facts need explaining](#)

[Lesson 3: Estimations. Predictions need an explanatory model as well as sufficient data](#)

[Lesson 4: Strategic notice. We do not have to be so surprised by surprise](#)

PART TWO: THREE LESSONS IN CHECKING OUR REASONING

[Lesson 5: It is our own demons that are most likely to mislead us](#)

[Lesson 6: We are all susceptible to obsessive states of mind](#)

[Lesson 7: Seeing is not always believing: beware manipulation, deception and faking](#)

PART THREE: THREE LESSONS IN MAKING INTELLIGENT USE OF INTELLIGENCE

[Lesson 8: Imagine yourself in the shoes of the person on the other side](#)

[Lesson 9: Trustworthiness creates lasting partnerships](#)

[Lesson 10: Subversion and sedition are now digital](#)

PART FOUR

A final lesson in optimism

Acknowledgements

[Notes and further reading](#)

[Index](#)

About the Author

David Omand was the first UK Security and Intelligence Coordinator, responsible to the Prime Minister for the professional health of the intelligence community, national counter-terrorism strategy and 'homeland security'. He served for seven years on the Joint Intelligence Committee. He was Permanent Secretary of the Home Office from 1997 to 2000, and before that Director of GCHQ.

For Keir, Robert, Beatrice and Ada, in the hope that you will
grow up in a better world

‘One of the best books ever written about intelligence analysis and its long-term lessons. Brilliant, lucid and thought-provoking’ Christopher Andrew, author of *The Defence of the Realm: The Authorized History of MI5*

‘An invaluable guide to avoiding self-deception and fake news. Unlocking the secrets of spycraft tells us something darkly important about ourselves. A sane antidote to some of the bewildering insanities of the age’ Melanie Phillips, *The Times*

‘This is nothing less than the new manual for analytical thought. What does it take to think clearly and maintain an open mind in the face of confusion? David Omand’s book *How Spies Think* prepares us for the challenges of the twenty-first century’ Richard J. Aldrich, author of *GCHQ*

‘Omand thinks and writes deeply about the intellectual and moral problems thrown up by a business that depends on stealing other people’s secrets. He knows what he is talking about. *How Spies Think* is engagingly readable, even though the arguments are complex ... The growing body of serious writing by professionals such as Omand helps to demystify, illuminate and keep honest a profession around which fantasists have always buzzed like flies’ Rodric Braithwaite, *Spectator*

‘A thoughtful handbook on the modern business of spookery’ *Financial Times*

‘David Omand has a unique combination of experience as both a producer and consumer of secret intelligence, a deep knowledge of intelligence history and techniques, and a gift for lucid exposition. An invaluable book for anyone who wants to think like a spy, but also for those concerned about the role spies can play in a democracy’ Lawrence Freedman, author of *The Future of War*

‘A rare insight into the methods and mindset of modern intelligence, written by a former top professional. A most valuable work’ Lionel Barber, author of *The Powerful and the Damned*

‘David Omand has more experience of the intelligence agencies and how they operate than anyone else in Britain. He also has the rare ability to explain spycraft and how raw intelligence is analysed without the use of jargon which would be incomprehensible to most readers. I have been waiting for a book like this for years’ Sir Malcolm Rifkind, former Defence Secretary and Foreign Secretary

‘A brilliant book, by one of the UK’s true polymaths – author, academic, administrator, mathematician – and former spy. But this isn’t just a book for those interested in the secret world of MI5, MI6 and GCHQ; it’s for anyone wanting to know how to make better decisions, and avoid the traps into which businesses and governments can, and do, fall, time after time’ Rt Hon. Jack Straw, former Home Secretary, Foreign Secretary and Lord Chancellor

‘Professor Sir David Omand deconstructs then reconstructs an important mode of thinking, spy thought, for those of us who deal with strategy, information, misinformation and disinformation. He leaves the reader with a powerful framework to help us face the realpolitik of the world’ Professor Michael Mainelli, Alderman and Sheriff of the City of London

‘*How Spies Think* is a masterclass in miniature form, offering the enduring lessons of a consequential life in service as keys to success in any profession facing the challenges and opportunities of an uncertain future’ Chris Inglis, former Deputy Director of the NSA

‘A tour de force. David Omand equips the reader with powerful intelligence techniques to survive in the new digital age. He lightens it with a fascinating selection of anecdotes, some first-hand, to illustrate his themes. And he makes an overwhelming case for rationality as the best response to a world of fake news and cyberattacks. Essential reading’ Richard Wilson, former Head of the Home Civil Service

‘With today’s political reality trumping political fiction, we rely now for mystery on the world of spies, espionage and secret intelligence. In this fascinating and revealing book David Omand, after a lifetime in that shadowy world, pulls back the curtain on spying triumphs, the occasional disasters, but also the important lessons for all of us from these dark but essential arts. It is a true eye-opener on a world which outsiders only guess about’ Lord George Robertson, former UK Defence Secretary and Secretary General of NATO

‘A fascinating book about how to think. Not just about intelligence but also about disinformation, distortion, subversion and all the other perils of a digital age. There cannot be anybody in Britain who can match David Omand’s broad experience in seeking, assessing and using secret intelligence. This personal experience produces his careful and thorough analytical rules’ David Wilson, Baron Wilson of Tillyorn, former Governor of Hong Kong

‘Britain’s spooks are world-renowned. This brilliant book lets us in on one of the secrets of their success – how to use rigorous analysis to separate fact from fake. It’s a skill that can help us all to make better choices in our lives’ Peter Ricketts, former British National Security Adviser

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 an 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. Harbours 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 decisionmaking 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

image

not

available

image

not

available

Lesson 1: Situational awareness Our knowledge of the world is always fragmentary and incomplete, and is sometimes wrong

London, 11 p.m., 20 April 1961. In room 360 of the Mount Royal Hotel, Marble Arch, London, four men are waiting anxiously for the arrival of a fifth. Built in 1933 as rented apartments and used for accommodation by US Army officers during the war, the hotel was chosen by MI6 as a suitably anonymous place for the first face-to-face meeting of Colonel Oleg Penkovsky of Soviet military intelligence, the GRU, with the intelligence officers who would jointly run him as an in-place agent of MI6 and CIA. When Penkovsky finally arrived he handed over two packets of handwritten notes on Soviet missiles and other military secrets that he had smuggled out of Moscow as tokens of intent. He then talked for several hours explaining what he felt was his patriotic duty to mother Russia in exposing to the West the adventurism and brinkmanship of the Soviet leader, Nikita Khrushchev, and the true nature of what he described as the rotten two-faced Soviet regime he was serving.¹

The huge value of Penkovsky as a source of secret intelligence came from the combination of his being a trained intelligence officer and his access to the deepest secrets of the Soviet Union – military technology, high policy and personalities. He was one of the very few with his breadth of access allowed to visit London, tasked with talent spotting of possible sources for Soviet intelligence to cultivate in Western business and scientific circles.

Penkovsky had established an acquaintance with a frequent legitimate visitor to Moscow, a British businessman, Greville Wynne, and entrusted him with his life when he finally asked Wynne to convey his offer of service to MI6. From April 1961 to August 1962 Penkovsky provided over 5500 exposures of secret material on a Minox camera supplied by MI6. His material alone kept busy twenty American and ten British analysts, and his 120 hours of face-to-face debriefings occupied thirty translators, producing 1200 pages of transcript.

At the same time, on the other side of the Atlantic, intelligence staffs worried about the military support being provided by the Soviet Union to Castro's Cuba. On 14 October 1962 a U2 reconnaissance aircraft over Cuba photographed what looked to CIA analysts like a missile site under construction. They had the top secret plans Penkovsky had passed to MI6 showing the typical stages of construction and operation for Soviet medium-range missile sites. In the view of the CIA, without this information it would have been very difficult to identify which type of nuclear-capable missiles were at the launch sites and track their operational readiness. On 16 October President Kennedy was briefed on the CIA assessment and shown the photographs. By 19 October

he was told a total of nine such sites were under construction and had been photographed by overflights. On 21 October the British Prime Minister, Harold Macmillan, was informed by President Kennedy that the entire US was now within Soviet missile range with a warning time of only four minutes. Macmillan's response is recorded as 'now the Americans will realize what we here in England have lived through these past many years'. The next day, after consultation with Macmillan, the President instituted a naval blockade of Cuba.²

The Cuban missile crisis is a clear example of the ability intelligence has to create awareness of a threatening situation, the first component of the SEES model of intelligence analysis. The new evidence turned US analysts' opinion on its head. They had previously thought the Soviets would not dare to attempt introducing nuclear missile systems in the Western hemisphere. Now they had a revised situational awareness of what the United States was facing.

There is a scientific way of assessing how new evidence should alter our beliefs about the situation we face, the task of the first stage of the SEES method. That is the Bayesian approach to inference, widely applied in intelligence analysis, modern statistics and data analysis.³ The method is named after the Rev. Thomas Bayes, the eighteenth-century Tunbridge Wells cleric who first described it in a note on probability found among his papers after his death in 1761.

The Bayesian approach uses *conditional probability* to work backwards from seeing evidence to the most likely causes of that evidence existing. Think of the coin about to be tossed by a football referee to decide which side gets to pick which goal to attack in the first half of the game. To start with it would be rational to estimate that there is a 50 per cent probability that either team will win the toss. But what should we think if we knew that in every one of the last five games involving our team and the same referee we had lost the toss? We would probably suspect foul play and reduce our belief that we stand an even chance of winning the toss this time. That is what we describe as the conditional probability, *given* that we now know the outcome of previous tosses. It is different from our prior estimate. What Bayesian inference does in that case is give us a scientific method of starting with the evidence of past tosses to arrive at the most likely cause of those results, such as a biased coin.

Bayesian inference helps us to revise our degree of belief in the likelihood of any proposition being true *given* our learning of evidence that bears on it. The method applies even when, unlike the coin-tossing example, we only have a subjective initial view of the likelihood of the proposition being true. An example would be the likelihood of our political party winning the next election. In that case it might then be new polling evidence that causes us to want to revise our estimate. We can ask ourselves how far the new evidence helps us discriminate between alternative views of the situation or, as we should term them, *alternative hypotheses*, about what the outcome is likely to be. If we have a number of alternatives open to us, and the evidence is more closely associated with one of them than the alternatives, then it points us towards believing more strongly that that is the best description of what we face.

The Bayesian method of reasoning therefore involves adjusting our *prior* degree of belief in a hypothesis on receipt of new evidence to form a *posterior* degree of belief in it ('posterior' meaning after seeing the evidence). The key to that re-evaluation is to ask the question: if the hypothesis was actually true how likely is it that we would have been able to see that evidence? If we think that evidence is strongly linked to the hypothesis being true, then we should increase our belief in the hypothesis.

*image
not
available*

Index

The page references in this index correspond to the print edition from which this ebook was created, and clicking on them will take you to the location in the ebook where the equivalent print page would begin. To find a specific word or phrase from the index, please use the search feature of your ebook reader.

- 9/11 conspiracy thinking 142–6, 313nn13–14
- Able Archer exercise 187–8
- Adams, Gerry 195
- Admiralty 157
 - Room 40, Whitehall 157, 158, 212–13
- advertising technology 173, 240, 244–5, 261–3
 - and vloggers 266–7
- AI *see* artificial intelligence
- AIDS 169–70
- airlines, and Eyjafjallajökull eruption 89–91
- Al Qaid’a 54, 93
- Alexander, Hugh 213, 214
- ambiguity effect 124
- Ames, Aldrich 133, 192
- analysis of competing hypotheses (ACH) 57, 302n13
- analytical thinking
 - in intelligence *see* intelligence analysis
 - SEES model *see* SEES analysis
- Anaya, Jorge Isaac 85
- Andropov, Yuri 67, 69, 184
- Angleton, James Jesus 132–3, 134–8, 139, 142, 174–5, 216
- Apple Safari 36
- Architects and Engineers for 9/11 Truth 145
- ARCOS (All-Russian Cooperative Society) 171
- Argentine Junta 1–2, 12–13, 53–4, 78, 84–5, 91, 122, 164–6
- artificial intelligence (AI) 32, 46–7, 75, 240, 244, 267, 291
- Asimov, Isaac 293
 - Foundation and Empire* books 82–3
- Assange, Julian 161
- atomic research 215–16
- attentional bias 127–8
- Australia, 5-eyes partnership 210–11, 215
- auto-subversion 243–4
- automated visualization tools 300n9

Penguin

UK | USA | Canada | Ireland | Australia
New Zealand | India | South Africa

Penguin is part of the Penguin Random House group of companies whose addresses can be found at global.penguinrandomhouse.com.



Penguin
Random House
UK

First published by Viking 2020

Published with a new preface in Penguin Books 2021

Copyright © David Omand, 2020, 2021

The moral right of the author has been asserted

The passage on page 148 is taken from *Tinker Tailor Soldier Spy* by John le Carré, published by Penguin Modern Classics, 2018. Originally published by Hodder & Stoughton, 1974. Copyright © le Carré Productions, 1974. Reproduced by permission of Penguin Books Ltd

ISBN: 978-0-241-38520-3

This ebook is copyright material and must not be copied, reproduced, transferred, distributed, leased, licensed or publicly performed or used in any way except as specifically permitted in writing by the publishers, as allowed under the terms and conditions under which it was purchased or as strictly permitted by applicable copyright law. Any unauthorized distribution or use of this text may be a direct infringement of the author's and publisher's rights and those responsible may be liable in law accordingly.