Corporate Security Intelligence and Strategic Decision Making

Corporate Security Intelligence and Strategic Decision Making

Justin Crump


CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150312

International Standard Book Number-13: 978-1-4665-9272-8 (eBook - PDF)

CONTENTS

SECTION II Theory

FOREWORD

By David Burrill Obe

Intelligence expert and former Chief Security Officer

Corporate Security Intelligence is a fundamental part of the basis on which business security decisions should be made. Few would deny that this is a prerequisite for decision making and yet it is, sadly more often than not, treated with lip service. The need for threat and risk analysis, activities which depend on good and timely intelligence, to influence the delivery of security, corporate or otherwise, can be found in most security policies. Unfortunately, it is common to discover that such analyses are infrequently conducted and infrequently subjected to even the most rudimentary re-assessment. In short, key company decisions are therefore made on the basis of ignorance; ignorance of fact and ignorance of professional projections on future developments.

The impact of what I consider to be corporate negligence has significance way beyond what is traditionally, and wrongly, considered to be the narrow confines of corporate security measures. Good corporate security intelligence is crucial to, amongst others, the due diligence process required for mergers and acquisitions, to entering new markets, and to the management of crises.

The unfortunate picture that I paint is caused by amateurism on the part of corporate security departments, executive committees and boards, and all stakeholders focused on the enablement of business, the projection of outstanding reputation and governance of the highest standards. If they "do not get it," "it" being the potential return on investment of corporate security service which is underpinned by timely and accurate corporate security intelligence, then re-education is long overdue. A growing number of companies do take a professional approach. They set a benchmark against which weaker performances will be measured; informally for the most part but formally, sometimes in law, when weakness may be perceived in the aftermath of incidents, particularly major incidents, as being causal or responsible for inadequate mitigation.

Given the context that I have described, I am delighted that Justin Crump has decided to produce this timely work on corporate security intelligence.

I recommend it to all professionals in the field of security and risk, and to all stakeholders, especially key corporate decision makers. Most especially, I recommend it to all whom hither "have not got it." Given the world today, it is about time they did!

David Burrill

November 2014

David is the former deputy director Intelligence Corps and chief of staff of the Intelligence and Security Centre, UK Armed Forces. On leaving the military he became chief security officer of British American Tobacco. In more than twenty years of private sector work, he became president of the International Security Management Association; remains an emeritus member of the Risk and Security Management Forum; and was the first co-chairman of the UK Foreign and Commonwealth Office's Security Information Service for Business Overseas (SISBO)—a public/private sector partnership initiative of which he was one of the key architects.

David was awarded an OBE in the 2004 New Years Honours List for services to international security management. In 2005, David was honored by CSO Journal *with a Compass Award for visionary leadership, and by ASIS International as the first recipient of its European Leadership Award. In November of that year he also became the first foreigner to receive a distinguished achievement award from the Overseas Security Advisory Council of the US Department of State, and is the first foreigner to be granted alumni status of the distinguished council. Finally, in July 2006, he was recognized by the Association of Security Consultants with the award of the Imbert Prize for distinguished achievement from citations submitted by ASIS International, the British Security Industry Association, and The Security Institute. He remains highly active coaching, training and mentoring emerging leaders in the security field and also helping identify and drive action around emerging trends.*

INTRODUCTION AND ACKNOWLEDGMENTS

Despite a long history, the art and science of corporate security has long been a neglected topic, and the study of intelligence within this setting remains even more so. However, this trend is changing. The increasing size, scale, and sophistication of corporate activities on the world stage—coupled with increasing legislative attention—is driving an increasing focus on this topic area, and the traditional gap between "business" (which makes money) and "security" (a corporate cost center) is markedly narrowing.

It is perhaps hardly surprising that this topic should not traditionally have received the attention it deserves. After all, the wider issue of intelligence in the national security context, which has justifiably drawn much more academic and public attention, is in itself still poorly understood. Although most commonly included under political science, the study of intelligence cuts across a huge range of human endeavor, incorporating organizational science, psychology, business, literature, and drama, to name just a few areas of relevance. In a similar vein, the practitioner must be both an artist and a scientist, comfortable with working with words and numbers, and presenting both in written and verbal fashion; be a humble influencer; and be an introverted extrovert. Practitioners must be comfortable with failure and be able to overcome this and keep "kicking on"; they must similarly be at home with complexity and thrive in frustrating and uncertain environments. Moreover, they must be able and willing to put themselves forward and present a view that may be unpopular without taking reactions personally.

It is hard not to have respect for those who do this job in the public sector, where they are at least part of large apparatuses that provide structure, support, certainty of employment, clear career paths, and rigor. How much harder, then, to do this in the corporate or NGO sector, where few of these benefits apply! Corporate analysts will often be working solo, or in a very small team; may be seen ultimately as a cost to the business; and will constantly be evaluated as to their value and worth on the strictest of scales. There is no certainty of support or funding, and there

is no "fudge factor" to hide behind. Moreover, power and organizational structures are often shifting, and clients are won or lost on influence. The corporate intelligence practitioner—as with any responsible corporate security operator—must therefore be an astute business operator with a whole range of soft skills as well as the hard skills relevant to the trade.

The last few years have seen a renaissance in this industry, as the understanding of intelligence-led security operations seeps into the corporate sector. After all, intelligence drives efficiency in response and helps prevent threats from harming the company, its people, and its assets; protects them from harm; prepares them for possible threats; and ultimately drives profits through its support of management decision making at all levels.

This book therefore serves to address the current void of awareness about and study of the corporate security intelligence environment. It draws on the increasing volume of material relevant to national security intelligence work, but it also incorporates a great deal of personal and organizational experience gained supporting corporate clients worldwide through a variety of challenging circumstances. It has been supported by key members of the International Security Management Association (ISMA), which forms the worldwide association for chief security officers; by ASIS, the largest corporate security organization globally; and by the UK's Resilience and Security Management Forum (RSMF). I am also grateful to all members of the Analysts' Roundtable network, with many offering encouragement, stories, and support throughout the process of writing this book to specifically address the topic.

This work would not have been possible without the support of a great number of people. A number of more personal thanks are also in order, for those key individuals who have helped with this process. Firstly, to David Burrill for helping correct the first proofs and kindly offering to write the foreword. His lifetime of relevant experience has been a great help. All members of the Sibylline team have also been immensely helpful in providing support, encouragement and research/writing; particular thanks must go to Rick Moyes, Matthew Fribbance, Ashlea Cliff, Maria Fjeldstad, and Ollie Fairbank, all of whom provided excellent input at a critical time. Jonathan Dunbar, Peter Gordon-Finlayson and Helen Clamp also all provided extremely useful feedback during a very hectic summer, and very much helped get this book over the line. All are not just colleagues, but also friends, and I hope that in turn they will continue to find the lessons from the book useful.

Critically, I have to thank two wonderful American women. Firstly, Dr. Nicole Lipkin for planting the seed; supporting her as she wrote her second book was an eye-opening experience, which made this work possible. She taught me much. Liz Chamberlin meanwhile has been a support throughout and without her this would not have been achieved. It is strangely fitting that she was able to celebrate with me somewhere in mid-atlantic at 35,000 feet when the work was finally complete….

Last, but very much not least, fantastic thanks are due to the very supportive, patient, and encouraging team at CRC Press. Prudy, Suzanne, Kate, Jennifer, Shayna, Kathryn and Mark (who initially bought my pitch over coffee at ASIS—how long ago now) are all brilliant. I'm very grateful that they have helped bring the lessons of the last twenty years to life, and hope that the end result does them justice.

ABOUT THE AUTHOR

Justin Crump has been working in the risk, intelligence and analysis field for over twenty years. A graduate of Durham University and King's College London, he initially worked with the Conflict Studies Research Centre (CSRC), then based at the Royal Military Academy, Sandhurst, UK. As part of this work he was primarily responsible for examining the post-Cold War evolution of Russian maritime strategy. This included work on a number of varied and exciting projects for the Royal Navy, and has fueled a lifelong interest in Russian military capability.

In 1998 Justin gained employment with Chase Manhattan as an Investment Banking analyst, based in London, Geneva and New York. Following a highly intensive training program—equivalent to a degree in banking in just four months—he rotated between departments including Mergers and Acquisitions; Financial Sponsors Debt Capital Markets; and the Chase Private Bank. This period saw a great deal of fluctuation in emerging markets, including the Argentine default and Russian crash, and so this was a particularly fascinating time to help clients negotiate these issues.

The events of September 11, 2001 drove a radical change in Justin's career. Having joined the British Reserve Forces in 1995, he volunteered for full-time service and was mobilized to the Queen's Royal Hussars, an armored regiment equipped with the Challenger 2 tank. By November 2001 he was therefore deployed on operations in the Balkans, initially serving as a staff officer in Regimental Headquarters, before taking over a troop in the Brigade Operations Squadron—specialized group undertaking operations across the north-east of the country.

Following the successful completion of this tour, Justin undertook advanced technical training on the Challenger 2 before taking over a tank troop in Germany. This involved intensive training to support operations in Iraq, including learning Arabic to a colloquial level, before deploying to

the country in late 2003. This operational tour initially saw Justin assume responsibility for reconstruction and development of a swath of territory north of Basra, but in early 2004 he was moved to Maysan to support the police force; during this period he saw firsthand the failure of policies, especially regarding the Shia militias, as a result of which he saw weeks of combat in and around the provincial capital, al-Amara.

On return from Iraq Justin joined PA Consulting, the leading UK management consultancy. During this period he was involved in the development of national security programs which remain classified. This involved exposure to both human and technical aspects of intelligence work, which influenced his subsequent career. However, he also had a role as the Aide to Major General the Duke of Westminster KG, the first Reservist officer of that rank since before the Second World War. The General was immensely active, helped by his private resources, and so Justin was soon called to focus on this role full time. From 2004–2007 he was therefore based in the Ministry of Defence in Whitehall, having exposure to policy at Ministerial level during a particularly interesting and critical time. The role also involved an extensive overseas visit program, giving the opportunity to meet key senior foreign personalities and develop relationships. A particular focus were continued protracted visits to operations in the Balkans, Iraq and Afghanistan, where Justin was able to spend time on the ground in Kabul and Kandahar.

In 2007 Justin returned to civilian life, becoming a country risk analyst for the niche British consultancy Stirling Assynt, working alongside a number of former senior intelligence officers. This role saw him embedded with Unicredit, the leading Italian bank, based in Milan. In recognition of his performance, he was promoted in 2008 to become Head of Threat Intelligence, running all the firm's routine analytical output. This saw responsibility for developing a fast-growing team, with offices in London and Hong Kong, and analysts embedded in a number of major companies. In 2010, the firm's analysis was featured in an exclusive report on the front page of the *South China Morning Post*, which led almost overnight to Justin being in demand as a media commentator, focusing on intelligence affairs. This has included being invited to be a blogger on security and intelligence for the *Huffington Post*, and he routinely appears on international news channels, both as an expert commentator and during topical debates, where he has appeared alongside senior government figures.

Justin founded his own successful firm, Sibylline Ltd, in 2010 with the aim of focusing more on emerging areas of intelligence in the corporate environment. This includes aspects such as cyber operations and social

media collection, as well as developing the approach and theories outlined in this book. Sibylline now supports a large number of companies, ranging from blue chips to medium-sized enterprises, as well as governments, and since 2010 Justin has built the company up in line with his vision to professionalize corporate intelligence work. The firm also runs the Retail Industry Security Centre in the US, providing threat information to hundreds of malls; retail chains; and law enforcement personnel nationwide, In 2011, this work led Justin to be invited to brief the main gathering of the State Department's Overseas Security Advisory Council Annual Briefing. He is a regular speaker at industry conferences, including regional OSAC meetings, as well as for ISMA—the leading association for Chief Security Officers. This experience both reflects and maintains Sibylline's position as thought leaders in corporate intelligence.

In 2013 Justin became Head of Intelligence for the ANVIL Group, following a strategic partnership with Sibylline. He also supports the not-for-profit City Security Resilience Networks (CSARN), a business and security networking and briefing organization founded by leading figures in the UK security industry. In what is laughingly called "spare time," he continues to serve as a Reservist, currently having the great privilege to command a Challenger 2 Squadron based in the south-west of the UK.

Section I

Rationale

1

What Is Corporate Security Intelligence?

Understanding how to act under conditions of incomplete information is the highest and most urgent human pursuit.

Nassim Nicholas Taleb (2007)

CHAPTER OBJECTIVES

1. To understand what is meant by the term *intelligence* in the corporate security environment.
2. To illustrate basic details of the background, history, and development of intelligence as a corporate function.
3. To understand the continuing evolution of security intelligence in the corporate environment and the concept of Enterprise Management.
4. To recognize how intelligence relates to strategic decision making, who the audience is, and what the function can and cannot offer.
5. To comprehend the value of *decision advantage* and gain an initial understanding of how this can be achieved.

INTRODUCTION

Intelligence is a defining function of human existence, and it has driven the rise and fall of empires and enterprises for thousands of years. Indeed,

this is a function that is as old as recorded history, and sometimes it lays claim to being the oldest profession. Yet it remains a remarkably poorly understood topic, long being regarded more as an art than a science, and generally a "dark art" at that. Although increased accountability and openness among Western governments has raised public awareness and understanding of at least some of the factors underlying the intelligence production process—helping somewhat to dispose of the myths, legends, and suppositions driven mainly by Hollywood and the media—attention has almost exclusively focused on governmental bodies and processes. In contrast, the role of intelligence in relation to corporate security—or otherwise residing in the private sector—has received very little attention. This reflects a comparatively disordered approach to the application of intelligence in corporations and nongovernmental organizations, with no standards or models being applied; consequently, structures, roles, responsibilities, and accountability vary widely.

However, a variety of push and pull factors are currently greatly increasing the level of interest in both corporate security and intelligence within the private sector. Private security intelligence contractors to the formal US intelligence community (IC) have probably drawn the most attention, with a series of exposés in the *Washington Post* since 2010 showing the significant scale and capability offered by these vendors. This is because such firms can offer niche expertise, "surge" personnel, and in some cases very cost-effective solutions to problems. Such features also make private security intelligence providers increasingly appealing to corporations, and increasing awareness of the potential offered by a security intelligence function has driven the establishment of internal posts reflecting this role (a topic we will return to in the following chapters).

INTELLIGENCE DEFINED

Given the general misunderstandings over the nature of corporate security intelligence, it is important to start any discussion with some basic definitions (a prelude to the theory that follows later in this book). The first thing is to understand the meaning of the actual word *intelligence* when used in this context. As mentioned previously, it is a term that is increasingly bandied around. In common use, it can refer to any of the following:

- Product
- Process
- Structures that carry out process and generate product

This can occasionally cause confusion. The most important underlying point, though, is to understand a single thing: Intelligence and information are different. Information surrounds us, but mainly in the form of raw data, lacking context or coherence. By contrast, the intelligence product is material considered and refined to produce insight. This difference highlights why the increasing volume of data now available to us in the digital age is, in fact, one of the reasons why intelligence is becoming more popular as a corporate issue.

Defining exactly what is meant by the term *intelligence* remains a matter of some dispute, even among the intelligence community (IC). Various recent definitions are listed in the accompanying sidebar. These definitions are mostly written to suit the agency or department concerned, but one key and clear point emerges: This is material designed to support the decision maker at all levels (strategic, operational, and tactical). One way to approach this is to consider that intelligence material generates context and understanding that allow people to better evaluate the likely shape of the current situation as well as the impact and likelihood of events.

VARYING DEFINITIONS OF INTELLIGENCE

The term foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons.

U.S. National Security Act of 1947, Section 3, p. 6.

Intelligence deals with all the things which should be known in advance of initiating a course of action.

Commission on Organization of the Executive Branch of the Government (The Hoover Commission, 1955), Intelligence Activities, p. 26.

The ability to apprehend the interrelationships of presented facts in such a way as to guide action towards a desired goal.

Luhn, H. P. 1958. A business intelligence system. *IBM Journal of Research and Development* 2 (4): 314.

Intelligence is knowledge of the enemy.

Troy, T. F. 1991. The "correct" definition of intelligence. *International Journal of Intelligence and CounterIntelligence* 5 (4): 447.

Intelligence is secret, state activity to understand or influence foreign entities.

Warner, M. 2002. Wanted: A definition of intelligence. *Studies in Intelligence* 6 (3): 21.

Intelligence, then, is a process, focused externally and using information from all available sources, that is designed to reduce the level of uncertainty for a decision maker.

Wheaton, K. J., and M. T. Beerbower. 2006. Towards a new definition of intelligence. *Stanford Law & Policy Review* 17 (2): 329.

The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

Department of Defense. 2010. *Dictionary of Military and Associated Terms*, 143. Washington, DC: Skyhorse.

We define business intelligence as the leveraging of a variety of sources of data as well as structured and unstructured information to provide decision makers with valuable information and knowledge. These sources of information and data could reside within or outside the organization, and the information and data could be either quantitative or qualitative.

Sabherwal, R., and I. Becerra-Fernandez. 2011. *Business Intelligence*, iii. New York: John Wiley & Sons.

Information acquired against the wishes and generally without the knowledge of the originators or possessors. Sources are kept secret from readers, as are the techniques used to acquire the information. Intelligence provides privileged insights not available openly.

United Kingdom Secret Intelligence Service. Definition of Secret Intelligence. sis.gov.uk.

> Competitive Intelligence is a necessary, ethical business discipline for decision making based on understanding the competitive environment.
>
> *Strategic and Competitive Intelligence Professionals*. scip.org.

The closest accepted corporate parallel is the field of *knowledge management*, although a key difference is that intelligence material should be responsive and proactive. *Timeliness*, *accuracy*, and *relevance* are often cited as important factors in producing good material, but the most important aspect—and the greatest difference from the collection of information or even knowledge—is that intelligence should be *actionable*. Although many in the public sector IC do not regard this as a precondition, in the corporate environment, the need to show return on investment (ROI) and similarly respond to financial pressures means that to produce something otherwise is an almost unheard of luxury. Therefore, the fundamental essential feature of corporate security intelligence is that it be of use to the decision maker at whatever level is required (be that tactical, operational, or strategic).

INTRODUCING DECISION ADVANTAGE

The point of intelligence, as outlined previously, can be partly summed up in a pithy little term that we will return to again and again in this work: It is to create what is known as *decision advantage*. This term was originally coined by Jennifer E. Sims, director of intelligence studies and visiting professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. It gained more mainstream awareness after the director of national intelligence referred to it in the 2008 publication *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*. He described the need to gain an edge in terms of information or insight, which "can dissolve a decision-maker's quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence."

Professor Sims originally used the term to refer to operations in an international relations environment, i.e., by state actors, and it is usually used in this context. However, the essential underlying idea of

intelligence as a lubricating aid to smooth strategic decision making is of course equally applicable to the corporate environment. Indeed, corporations routinely seek decision advantage in the marketplace, and they have highly sophisticated mechanisms for doing so. The concept, if not the term, should therefore be familiar to most senior executives.

THE CORPORATE SECURITY ENVIRONMENT

So, if we accept this basic understanding of what intelligence offers and is seeking to achieve, our next task is to understand how this applies within the field of corporate security. This issue is going through a highly significant evolution at present, driven by the threat environment as well as business factors. There is a very distinct move away from security being about almost janitorial functions ("doors and windows") and coinciding with increasingly positive perceptions of the importance of security to businesses. Again, no two definitions would be the same, but the following activities are the main possible pillars of a corporate security function in the second decade of this century:

- Physical protection of assets
- Physical protection of people
- Business continuity
- Crisis response/management
- Cyber security
- Information and data protection
- Internal investigations
- Countering fraud and money laundering
- Counterespionage
- Brand protection
- Anticounterfeiting/piracy

These represent a reaction to the main threat groupings that exist to challenge companies in the current environment, and we will examine each of these in more detail in Chapter 3.

In practice, these functions rarely sit within one department, and every company is different. Moreover, our basic definition of *intelligence* is clearly not limited to these security-linked activities, even if this is where it is most perceived to exist as a separate subject. Again, many firms may already have particularly advanced "intelligence" processes, generally directly related to their market or competitors (with *decision advantage*

being the usual objective). These are, however, not termed or recognized as such—something that begs the question of whether all parties are missing a trick and whether a clearer understanding and application of intelligence theory across the enterprise would help integrate security even further.

THE HISTORY OF CORPORATE INTELLIGENCE

Despite the comparative lack of published work on the subject, as with spying in general, corporate intelligence is not in any way a new phenomenon. As discussed previously, awareness of the market and competitors is probably a function that began when someone opened the second-ever commercial enterprise. Even in the field of security, examples can be readily traced back to the seventeenth century, which saw the rise of the Dutch and British East India companies. These early corporations had huge armed wings for self-defense, which eventually even became tools of conquest. For example, Britain's Honourable East India Company provided much of the garrison of India in the early- and mid-nineteenth century. Their corporate structures were entire apparatuses for the collection of information that was directly (albeit informally) related to decision making.

As the forces of the East India companies mirrored national armies, so their intelligence capabilities reflected contemporary military thinking. This included somewhat exotic views of intelligence as a topic, with many regarding spying as being "unworthy of gentlemen." From its inception, the United States has made good use of spies during times of conflict. Indeed, the statue of patriot Nathan Hale, caught and killed on a mission behind British lines during the Revolutionary War battle of Long Island, stands as a memorial in the CIA headquarters in Langley, Virginia. However, this capability was always allowed—if not positively encouraged—to languish between conflicts, perhaps in part due to some of the ideals on which the nation was founded. In contrast, the colonial interests of European powers encouraged more of such activity, and in a more scientific fashion, notably during the "Great Game" of maneuvering for influence in South and Central Asia. Nevertheless, the topic was still much more in the realm of art, largely inspired by individual acts of genius.

As with so many other acts of human endeavor, the beginning of industrialization began to drive a formalization of these sorts of processes. The American Civil War can, in many ways, be regarded as the first truly modern conflict. In the time leading up to that war, a particular

corporate security intelligence provider rose to the fore: the Pinkerton's National Detective Agency, founded in 1855. Alan Pinkerton initially established this firm to serve the desires of several employers (mainly railroad companies), who wished to exercise greater oversight and control over their employees, and who felt that an outsourced company could best suit their needs. The company rose to prominence as an important part of the Union's intelligence apparatus, and Pinkterton acted as a staff advisor to General McClellan, playing an important (albeit fatally flawed) role in the Peninsula Campaign of 1862. Pinkerton's claim to have foiled a plot against Abraham Lincoln resulted in his detectives being employed to guard the president during the war, and the company assumed a series of other quasi-military roles in support of the war effort.

The Pinkerton Agency continued to gain strength after the conflict ended, and the agency played a major role in strike-busting activities during the 1870s, 1880s, and 1890s. In 1892, these activities led to clashes with workers that resulted in deaths on both sides, and eventually there were calls for the company's power to be restricted (showing that concerns over the reach of private intelligence companies working alongside the state are not entirely a phenomenon of the modern, post-9/11 environment). Other rivals emerged—most famously the William J. Burns Detective Agency—and by 1937 the company had ceased to operate against the unions, reflecting evolving priorities. By the 1960s, the term *detective* was dropped from the title and, following a 2003 acquisition by the international security services giant Securitas AB, the company—still in operation—became known as Pinkerton Consulting and Investigations.

Although few records have been kept, the likelihood is that many companies employed a form of security intelligence capability as a result of the increased industrialization—and resulting tensions—of the mid-nineteenth century onwards. After all, if there was an outsourced service that was so much in demand, it is more than likely that some chose to take this work in-house. Given the priorities of that age, and the impact on the bottom line, industrial relations were almost certainly one of the issues closest to management's heart, and it is almost certain that this, rather than the safety of employees, would have been a major task for the nascent intelligence function.

The gradual professionalism of intelligence as a science in Western nations was demonstrated in the run-up to the First World War. The first decade of the twentieth century saw increasing awareness of espionage in the public consciousness, with some classic spy novels such as Erskine Childers's 1903 work *The Riddle of the Sands* reflecting the wider mood.

In 1909, the United Kingdom took a significant step by forming the Secret Service Bureau, initially a joint army–navy unit; the army component was focused on preventing German espionage, while the naval section predominantly aimed to gain intelligence on the Kaiser's fleet. With the outbreak of war, these split into the Directorates of Military Intelligence 5 and 6, respectively. MI5 and MI6 live on as colloquial terms for these two services, which remain in operation today as the Security Service and Secret Intelligence Service of the British state.

Although not corporate in nature—albeit by the Cold War their role had evolved to support British and allied businesses—the formation of this sort of permanent function within government in peacetime was a radical step toward enshrining intelligence as a science. The United States remained more resistant to change: The FBI was not set up until 1937, and initially it had no intelligence function. It took the experience of the Second World War for Washington finally to accept the need for a permanent apparatus. In 1947, this led to the establishment of what has now become the CIA.

Again, although records are not entirely clear, the increasing professionalism of intelligence in the public sector would have had a knock-on effect in the private sector, especially as security staff were mainly recruited from "connected" ex-agency or police staff. However, outside the FBI, the acceptance of intelligence in police circles has been a slow process, in part driven by the requirements to react to crime rather than seek to preempt it. This did not change until the early 1990s, when the Kent Constabulary of the United Kingdom realized that, by adopting an intelligence-led approach, they could track back and destroy organized crime networks "at source" rather than just treating the symptom. This experience has since resulted in the adoption of the National Intelligence Model, which is copied and used by law enforcement agencies and police forces worldwide. Given the average length of career and the seniority of ex-police appointees to corporate security, the intelligence-led approach is only now seeping more widely into the industrial sector. Nonetheless, sufficient time has now elapsed for this to be a major driver for the revolution that is occurring in regard to the topic. Recent arrivals into the corporate sector now consider intelligence to be a critical driver for operations.

Of course, this history is very Western oriented. As with so many new theoretical inventions, the truth is that basic lessons keep being relearned through history. The embarrassing truth remains that many of the maxims and principles considered to be "emerging thought" are in fact just more structured ways of enacting the lessons encapsulated by the

writings of the Chinese general Sun Tzu, who is widely considered to be the author of *The Art of War*, a treatise written around 500 BCE, in a format common to Chinese generals. This work was a precursor to today's doctrinal pamphlets. Basic truisms of warfare are reflected throughout, and the last of the work's thirteen chapters reflects exclusively on the use of intelligence. The parallel between war and business as spheres of human group/social struggle was a premise of a later key strategic thinker, Carl Von Clausewitz (1780–1831), who stated in his seminal work *On War*:

> Rather than comparing [war] to art we could more accurately compare it to commerce, which is also a conflict of human interests and activities; and it is still closer to politics, which in turn may be considered as a kind of commerce on a larger scale.

Of interest is that numerous recent business books have used the principles of Sun Tzu to illustrate winning commercial strategies. *The Art of War* is reportedly required reading for executives in many Japanese firms, which raises the happy thought that the basic principles of intelligence should be well understood and applied in commercial life: so much the better for the modernization and acceptance of corporate security intelligence as a function.

A TYPICAL CORPORATE SECURITY DEPARTMENT

So, from the general history and application of this topic, let us move on to look at the apparatus within which the intelligence function must operate. Of course, as stated previously, the first thing is once again to acknowledge that there is no such thing as a typical corporate security department. The structures that exist have nearly always grown organically and can be heavily constrained by wider corporate hierarchies, geographical limitations, or confused reporting chains. Despite the best efforts of leading corporate security professional bodies such as ASIS International (formerly the American Society for Industrial Security), models also vary widely between companies, even between nearly exact competitors in the same industry, depending largely upon historical development and the characters of individual senior actors and influencers.

The following discussion reflects mainly upon multinational or larger US companies. These corporations generally tend to be made up of a large top-level entity—"the group"—with a series of divisions or subcompanies beneath it. Terms for these, and the scale, may change, and much depends

on the area of operation in terms of what legally constitutes each entity. However, the model applies across a surprisingly large range of conditions. For example, mall operators in the United States may be one legal entity, but operations are often broken down regionally, under a central head office. International banks similarly have a central head office, but, for legal and regulatory reasons, have a separate entity in each country where they operate. Business divisions based on industry groups or activities provide another common breakdown of corporations below group level.

Under the group structure, security generally tends to be focused at different levels. The chief security officer (CSO) or equivalent normally reports to a board member, often in line with other facilities-orientated services (although this is a weakness that does not reflect the full value of security as a business enabler); other possibilities are that security sits alongside legal or compliance functions, often within the human resource (HR) category. The CSO's immediate team tends to consist of heads of various functional areas within security, e.g., fraud, information security, physical security—which often includes executive protection—and potentially business continuity/crisis management. Their role is often the establishment and coordination of approach and policy, which is no small matter across highly complex structures. Operational delivery tends to be focused on the higher levels, or in support of centralized functions, such as group mergers and acquisition (M&A) activity or support to board-level operations. This is most commonly where a strategic intelligence function will sit, ideally reporting to the CSO directly. Under this model, much of the operational level of security is carried out by security teams belonging to business divisions/legal entities/other subordinate structures, with delivery of guards and so on often being delegated and subcontracted.

Small and medium-sized enterprises (SMEs) may well follow this structure. However, of necessity, all of an SME's business functions tend to be more directly aligned to purpose, or otherwise condensed. SMEs are therefore more likely to have at most a single small department looking at security, which more often than not will be merged with facilities. It is actually particularly likely that security functions in an SME will be spread across a number of people who hold other responsibilities, for example HR, rather than being focused in one person or team. This again reflects necessity, but it raises the irony that the firms that could perhaps most benefit from an intelligence-led, efficient model are those least orientated or able to adopt such an approach.

It should therefore be noted that while much of the discussion that follows, and throughout much of this book, will concentrate on the

multinational environment, the lessons are nonetheless equally applicable to SMEs. However, application will require a revision to the way that many smaller firms view security and business resilience—something that Western governments are on somewhat of a crusade to achieve, driven by the experience of recent security events. For example on December 11, 2005, the Total/Texaco-operated Hertfordshire Oil Storage Terminal located in Buncefield, UK, experienced a series of explosions seemingly caused by uncontrolled vapor release. The blast caused extensive damage to neighboring office buildings, although, thankfully, few injuries resulted due to the timing. Local infrastructure was otherwise greatly affected. However, beyond the immediate effects lay a bigger problem: Some of the comparatively small companies seriously affected by the blast had surprisingly important dependencies for much larger businesses. This sort of effect was not being modeled by traditional resilience/business-continuity exercises, which did not adopt a "systems approach" able to identify these sorts of emergent factors following an incident. This is due, in part, to the adoption of just-in-time production methods, a high degree of dependency on outsourced services, and the huge reliance on modern communications methods for most businesses to function. Similarly, the fact that offices were so near the storage facility reflects the increasing pressure on space for development, a factor that has also led to greatly increased development in areas prone to natural disasters (e.g., earthquake zones) since the second half of the twentieth century. On top of that, businesses are ever more global, and the counterpoint to the increased ease of travel and availability of opportunities is the fact that the globe is becoming a much, much riskier place. In this context, the necessity to increase resilience is pressing, but understandably, given the difficult economic climate and multitude of developmental challenges faced by SMEs, this is not viewed as a priority.

CHALLENGES TO EFFECTIVE CORPORATE SECURITY

Real corporate security faces serious challenges. First and foremost is that security is seen as a cost center by businesses, rather than as a business enabler. On this basis, most senior decision makers will instinctively look to de-prioritize security expenditure where possible. Moreover, security is one of the few business functions that is actively seeking to put itself out of business, in effect, seeking to reduce security incidents and, thus, reduce the perceived need for security. Assessed logically, a highly

effective apparatus will have the effect of negating threats to such a large extent that the very lack of emerging issues may cause it to become a victim of its own success: In this situation, security expenditure could well be cut as a result of the perceived overspend in contrast to the scale of the possible problem. This can and does happen surprisingly often, although, as it is hard for any company completely to control and mitigate the security threats in its environment, the wisest leaders understand that lack of an emerging problem does not mean that there is another on right around the next corner.

A traditional problem has also been the somewhat self-contained nature of corporate security. Traditionally, this function has sat as something of a black box within the business, lacking real integration with other corporate functions (in part due to recruitment policies almost entirely favoring ex-military/police/agency, etc., rather than "business types"). Both executives and security professionals were complicit in this approach, which was perhaps well orientated to the more rudimentary security threats of the 1960s, but which is generally useless against today's sophisticated, networked, and "learning" opponents and challenges. Sadly, this antiquated "leave it to us" model is still in operation in all too many corporations. However, the best are learning and evolving, with positive results across the board.

OVERCOMING THESE CHALLENGES: THE "BUSINESS OF RESILIENCE"

> In an increasingly complex and fast-moving world, the successful companies will be those who can manage change effectively on an ongoing basis. Aligning security with the business, therefore, does not merely make companies safer—it is one of the most important sources of competitive advantage in the twenty-first century.

So states a 2006 paper by the London-based think-tank Demos, entitled "The Business of Resilience; Corporate Security for the 21st Century." Written by Rachel Briggs and Charlie Edwards (2006), both very experienced security researchers, the paper drew on significant inputs from companies including BAT, BP, British Airways, Control Risks, E.On, G4S Global Risks Ltd., HSBC, Kroll Security International, Prudential, QinetiQ, and Shell. It has become required reading for most senior security

practitioners, and it remains the most noteworthy work on the subject of optimal security structures and approaches for multinational businesses.

The paper begins by acknowledging two main facts:

1. Doing business has become more complicated, requiring, for example, the development of matrix structures and devolution of power toward local managers operating through trusted networks.
2. This has happened in the context of a much a more complex security operating environment (sometimes for the same reasons, such as globalization, that have themselves driven up the complexity of business).

We touched on these facts when discussing resilience and SMEs, with the conclusion being that business and security now go hand in hand. As Briggs and Edwards (2006) put it, the companies that are succeeding in this vision realize that "the challenge for corporate security is no different from that for any other function—they must keep pace with their company's changing business environment to ensure that how they work, what they do and how they behave reflect these realities." The paper goes on to draw out six characteristics of companies that are integrating security with the business to the overall benefit of the company, which are broken out in the sidebar for ease of reference.

SIX CHARACTERISTICS OF COMPANIES THAT ARE INTEGRATING SECURITY WITH THE BUSINESS

"The Business of Resilience" highlights the following characteristics of companies with effective security:

1. They understand that *security is achieved through the everyday actions of employees right across the company*. It is not something that the corporate security department can do to or for the company on its behalf, and its functional success is therefore dependent on its ability to convince others to work differently. This places emphasis on communication.
2. They recognize the *limitations of command and control approaches to change management*. Behavior is altered only by convincing, persuading, influencing, and explaining why a new way of working is in each person's interest. This requires

departments to work through trusted social networks, which places greater emphasis on people, management, and social skills than security experience.
3. They understand that *their role is to help the company to take risks rather than eliminate them, and to have contingencies in place to minimize damage when things go wrong*. Risk taking is essential to successful business, and corporate security departments must not behave as security purists whose work detracts from, rather than contributes toward, the company's goals.
4. They *embrace and contribute toward their company's key business concerns*, and as a result are *expanding the security portfolio significantly*. Corporate security departments now have responsibilities in areas such as corporate governance, information assurance, business continuity, reputation management, and crisis management. The term *resilience* now more accurately reflects the range of their responsibilities.
5. They *draw a clear distinction between the strategic and operational aspects of security management* and have created group corporate security departments to lead on strategy, leaving operational work to be carried out by business units. They all have a clear philosophy to guide their approach to security.
6. Finally, and most important symbolically, the corporate security departments that are leading the way have *abandoned old assumptions about where their power and legitimacy come from*. Their position does not rest on that which makes them different—their content knowledge—but on business acumen, people skills, management ability, and communication expertise. In other words, they have to compete on the same terms as every other function in the company.

Put simply, the major change required is for security to stop acting as a black box within the business. This tendency has been driven by the backgrounds of many in this field: Research has shown that the vast majority of corporate security heads in the United States still come from the military, police, or intelligence agencies, and less than a quarter have backgrounds in business before taking up the post. The means, methods, and mores of their old careers therefore tend to predominate, especially in companies with very large security functions, which can naturally perpetuate a divide from the business. Again, this did not used to matter

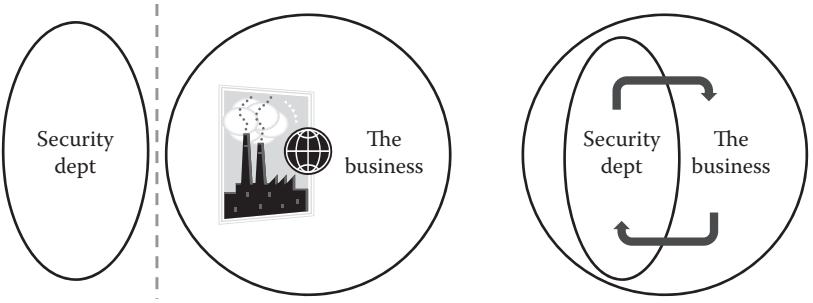

Figure 1.1 Comparison of "old" versus "new" corporate security models.

when the principal role was "doors and windows"—and perhaps passes. Now, however, the environment is changed, and the consequences of failure are far more damaging. Interestingly—and I speak as a product of such a system—a key difference between the military/intelligence/police and the contemporary business environment is that the latter is increasingly less hierarchical, opening up a real gap in experience (Figure 1.1). Emotional intelligence in particular is a subject that is almost anathema in the traditional security environment (being overshadowed by technical skills), but it is of vital and increasing importance in modern business.

THE ROLE OF INTELLIGENCE IN ENTERPRISE RISK MANAGEMENT

Enterprise Risk Management (ERM) is an increasingly popular accepted approach for identifying, analyzing, responding to, and monitoring risks and opportunities in the corporate operating environment. This brings together various processes for understanding and tacking risks, extending across the two dimensions of *risk type* and *risk management approaches*. This has developed extensively in the last ten to fifteen years, taking into account all the complementary but often separate activities that were being undertaken across different parts of organizations; for example looking at financial risk, the threat from regulatory changes, ethics and reputational issues, strategic planning, and examination of physical security problems. ERM seeks to integrate these areas, improving capability and

coordination across the organization, and helping it effectively visualize, manage and respond to risks and opportunities.

The increasing scrutiny of how corporations handle risk (of all kinds) has helped drive the adoption of ERM approaches. Regulation such as the Sarbanes–Oxley Act of 2002, stock exchange rules, debt rating agency approaches, and guidelines such as ISO 31000 (the International Risk Management Standard) all require the adoption of effective risk assessment in organizations. The result has been increasing focus at C-Suite level, with Chief Risk Officers or Chief Financial Officers being responsible for the delivery of ERM (and accountable to the CEO).

Obviously, ERM extends well beyond security. However, the integrated approach to risk means that there is a clear, financially costed, and resourced program for the security function to have input to. This also serves as a forum for discussing risks and brings the CSO into close contact with peers, improving their level of input into the organization (and further helping to overcome the "black box" model of security within the business). Moreover, this allows security risks and inputs to be placed clearly in a hierarchy of business risks, making security activities—and the value of such activities—more visible to the C-Suite.

Clear understanding of what matters to the organization also helps drive the priority for security matters. The value of intelligence around these sorts of clearly defined issues is readily apparent, and there is an increasing trend of security analysts moving upstream and helping to inform wider risk management approaches; this is especially the case as security users are well aware of the value intelligence brings in creating decision advantage, but this is not a capability that is familiar to e.g. legal or finance departments—and once they discover it, they're hooked. At least one S&P100 company now has intelligence analysts reporting directly to the CEO, and many others are adopting a wider process of intelligence around identified risks, including in the regulatory/political space (where the trick is often not being caught out by a potentially disastrous change in circumstances).

This is still an emerging theme, with many challenges to effective implementation. However, ERM is certainly here to stay, and the integration of risk awareness from across different "stovepipes" is doubtless a great step forwards in ensuring corporate resilience. Again, this has offered effective and forward-looking security departments the chance to shine, and really gain relevance and traction in their organizations at the highest levels. The extension of intelligence into new areas of the business

makes this a particularly exciting time for practitioners, and means the value of having an advanced and effective intelligence approach is currently greater than ever.

Although Briggs and Edwards (2006) did not break this out in the "Business of Resilience" paper, intelligence is clearly a key enabler to positioning security more effectively within the business. Insight is of vital importance to decision makers given growing risks and complexity, and despite—or perhaps because of—the plethora of information available, there is increasingly little actionable information discernible amongst the wider "noise." This can have a paralyzing effect on executives, or it can create symptoms almost akin to those of attention deficit disorder if not carefully managed. By providing timely relevant and accurate material, the intelligence function can give senior decision makers a sound platform on which to understand and address the problems and challenges they must confront. After all, as stated previously, the essential function of most businesses is effectively to price risk accurately; the company with better intelligence will in general make better decisions, whatever the market. Given the increasing riskiness of the global operating environment, with uncertainty being pervasive, this has recently taken on more importance than ever.

This environment is particularly challenging for the current crop of senior executives, who grew up in a world with more certainty in terms of both the economic and security climates. The security intelligence function therefore offers a critical, although often underappreciated, capability to support decision making and provide insight at the board level. In this regard, senior executives should be the main audience for the most strategic products from the intelligence function. This can be a hard sell at first to busy executives, but once a sponsor is found, then appreciation of the capability offered—and internal investment in its development and adoption—usually follows.

Within the security department itself, as we will go on to discuss in greater depth in later chapters, intelligence is in essence what the military terms a *force multiplier*. Against increasingly complex threats, conventional doors-and-windows models of security cannot hold up. Take IT security: The proliferation of networked devices under increasingly popular modern corporate "Bring Your Own Device" policies has resulted in even the most sophisticated and aware organizations struggling to understand where, exactly, their security perimeter is. As we will consider in Chapter 3, adversaries seek the weak joints in an organization, and the

crossover between physical security and cyber security additionally remains a major challenge. In this environment, the would-be attacker has a wealth of opportunities, and so comparatively scarce security resources need to be directed in the most effective manner possible.

This is another way of saying that intelligence makes for smarter, and thus more effective, corporate security. However, under this heading are a variety of more detailed reasons to use intelligence within the security function:

- To better focus finite security resources
- To inform the alert-level status
- To enable security to be proactive rather than reactive
- To provide an estimate of threat-response effectiveness
- To identify potential targets for in-depth investigation
- To validate an existing risk-management program
- To expose gaps in protection (vulnerabilities)
- To determine how effective a particular action has been in degrading an adversary's capability

Across the width of the organization, in addition to providing general material to provide context and support operational decisions, the need to tie into the emotional factor is an increasingly important driver. In difficult times, people at all levels seek reassurance, and emotional well-being can be just as important as physical safety. Given the proliferation of 24-hour news and social media, rumors spread quickly, and fears can rapidly be exaggerated, often increasing the level of concern for employees. Knowledge-based, calm, and informed analysis in these situations can do much to calm people in this sort of environment.

In this regard, it can be seen that sharing intelligence will benefit everyone, since, as the old proverb says, forewarned is forearmed. Ultimately, nowadays everyone in the company is a consumer at some level. Often, people in business will find a use for corporate intelligence information that may not ever have crossed the mind of the analyst(s) who worked on it. For example, the author has seen traders using travel security information circulating in a bank to help them price risk on commodities transactions—making the organization a lot of money in the process. This sort of use clearly helps strengthen the role of security in the business and brings the two into greater harmony, since this prompts the analyst to understand more about the wider business, making material more and more relevant.

CONCLUSION: TOWARD TRULY INTELLIGENT SECURITY AND BUSINESSES?

To summarize, the business environment is becoming ever more challenging in the face of multiplying threats, and the only thing that is certain is that there will be uncertainty—maybe. Against this background, security and resilience are becoming an integral part of being able to operate and compete effectively. The traditional preference for security practitioners with "hard" rather than "soft" skills has complicated this, but the best security departments are increasingly embracing the need to be adopted properly within the business—aligned with business function and processes—rather than sitting outside. This is still mainly happening only in the largest multinationals, but the adoption of best practice is being encouraged by industry groups and, indeed, is being shown in a plethora of practical examples, so now even SMEs are adopting a more sophisticated attitude toward risk and resilience.

In this climate, the advantages of intelligence are clear. Decision makers at all levels require timely, accurate, relevant, and actionable material to help them progress in the face of so many challenges. Increasing legal oversight and scrutiny, which we will consider in the next chapter, is further driving responsible development in this regard. Meanwhile, the plethora of information becoming available to employees at all levels has produced a need for analysis and real insight that is greater than ever. This requires the analyst(s) to know the business, and the business to know and trust the analysts, generating a cycle that brings security into ever closer alignment with commercial priorities, needs, and wants. Ultimately, the companies that use security intelligence to make intelligent decisions not only survive, but also tend to prosper in comparison to their competitors.

2

The Corporate Security Operating Environment

However absorbed a commander may be in the elaboration of his own thoughts, it is sometimes necessary to take the enemy into account.

Winston Churchill

CHAPTER OBJECTIVES

1. To understand the main current threats to Western companies, operating both domestically and internationally.
2. To outline how geopolitics, terrorism, cyber issues, espionage ("insiders"), single-issue activism, and crime affect the safe and security operations of companies and organizations both domestically and on the global stage.
3. To comprehend the main future and emerging threat trends of interest.
4. To gain initial insight into how security intelligence can be applied to these threats.

INTRODUCTION

The security operating environment of the twenty-first century presents a wide range of challenges to organizations. Traditional physical threats have been supplemented and, in some cases, supplanted by rapidly evolving electronic threats, and the boundaries of the enterprise have become ever harder to define. Moreover, as HSBC (Hongkong and Shanghai Banking Corporation) is fond of declaring in its advertising, in the future, even the smallest companies will operate globally. Ultimately, business is all about pricing risk, and in this regard, security risks are no different than any other.

This chapter therefore discusses some of the main operating threats to companies. There are of course others, but the areas outlined here are the ones that corporate security intelligence departments tend to focus time and effort on. In outline, these are as follows:

- Geopolitical risk
- Terrorism
- Cyber issues
- "Traditional" espionage and insider threats
- Single-issue activism
- Crime, including fraud and counterfeiting

These threats all continue to evolve and multiply naturally (of course, or else there wouldn't be much need for intelligence, and little point in reading the rest of this book). What follows is, of necessity, just an overview rather than a thorough analysis. However, it should suffice to offer an introduction to the topic for those just getting started in the field.

GEOPOLITICAL RISK

In today's business environment, corporations of all sizes need to concern themselves ever more with the threat posed by political events outside their control. No longer are internal and external political risks only an area of concern for those companies that choose to operate in emerging economies. Interconnectedness and such innovations as just-in-time production mean that the impact of politics on operations, markets, investment risk, and security is ever increasing. As a globalized, increasingly connected world presents companies with higher exposure to risk factors beyond their control, an understanding of those political factors is becoming ever more necessary.

Many of the political risks that a company faces are relatively minor but can be inconvenient if not properly predicted and dealt with. Simple, everyday operational concerns can be overturned by an often-predictable event or piece of legislation. Say, for instance, there is a change in visa standards for a company operating abroad. If dealt with in advance, this can be mitigated: The staff changes can be made, extra fees paid and worked into the financial model, and any necessary paperwork acquired can be managed. If such an event is predicted and implemented in a timely fashion, this should prove no problem for any reasonably organized company to deal with. If missed, it can leave crucial members of a team unable to enter their country to work. At this point, even small details become significant.

At the other end of the scale, firms face a severe downside risk from major political events that can absolutely undermine a company's operations in a short space of time. While theoretically rare, these scenarios play out more often than seems to correlate with standard distribution. These so-called long-tail risks can be devastating to a company. What is more, they are notoriously difficult to spot with standard statistical analysis. Major terrorist attacks, international conflicts, coups d'état, and civil disturbances are the most severe of these events. Expropriations, strikes, changes of government, or significant shifts in a country's political trajectory can prove equally threatening to profits, if less so to the lives of corporate employees. Understanding people (psychology) as well as dynamics is essential to prediction and mitigation of these risks; while economics treats people as rational actors, there is normally far more at play than pure cost–benefit analysis. To be done well, political risk analysis is therefore as much of an art as a science, especially given the complexity of the systems at work, which defy easy quantitative feedback.

Many boards assume that they can mitigate these risks by avoiding unstable markets, which is on the face of it a perfectly reasonable assessment. Avoiding potentially lucrative but risky markets may be a wise decision for organizations that are less able to handle the inherent challenges. However, changing times and increasingly competitive business environments have made these problems harder to ignore or avoid. For example, the later years of the last decade brought political risk clearly home to even the most stable and well-established economies. Bailouts and default fears across the Eurozone were not simply based on economics; these were political decisions, with confidence and corresponding bond yield swinging with prevailing sentiments from governments. Yet the economic costs to individual investments based on political decisions could be severe, bringing markets slumping with

reports of political impasse. With investments moving in recent years to the stronger but often less stable emerging markets, the price of failing to understanding political risk is clearly no longer limited merely to a few limited unstable dictatorships.

Unknown Unknowns

The biggest risk from geopolitics is those large-scale risks even professional risk analysts struggle to see coming, the end of the Soviet Union being just one example. These risks are not going away, and reliable knowledge, information, and intelligence is crucial to coming out of these developing situations in the best condition. Scenario analysis and having the ability to red-team the worst-case outcomes can be crucial to improving corporate survivability.

The Arab Spring provides a perfect example of a serious geopolitical event, almost entirely unforeseen, which ticks a number of the threat categories mentioned here. While countries across North Africa and the Middle East were unquestionably unstable and racking up social issues, there were very few who could have predicted the beginning of a regional upheaval. Companies with interests across the Middle East were suddenly plunged into a new environment. Political changes risking investments, the need to deal with new faces in government, strikes, protests, and civil wars threatening the safety of staff and assets and ruining economies suddenly affected countries that had been utterly stable and predictable for decades.

The risk of fuel price surges touched those well outside the region, while the possibility of contagion threatened governments near to affected countries, many of whom moved to both crush the protest and appease the population. The seeds sown during this upheaval are likely to be harvested over the next few decades. While the Arab Spring was a fine geopolitical long-tail risk, its effects by country are likely to vary vastly. Without necessarily seeing the precise event coming, good intelligence and strong networks and knowledge still allow the best possible response in what has been a fast-changing region since the start of 2011.

More obvious, isolated examples of political risk come from in-country events. Domestic risk certainly hasn't deteriorated in the last decade. In the most straightforward cases, in-country risks continue to emanate from the old places. Firms, particularly those with high sunk costs, continue to face expropriation risk, as in the case of Argentinean state oil company YPF, which was expropriated by the state from the Spanish firm Repsol in 2012.

Elections remain troublesome almost everywhere with the natural uncertainly they bring, but in some states they can prove particularly problematic. Overly obvious electoral fraud during the Russian parliamentary elections in December 2011 shook the system significantly, and the effects continue to be felt, with crackdowns souring the business environment. In Kenya, businesses and investors nervously waited for the country's supreme court to rule on the March 4, 2013, polls after contested elections in 2007 led to clashes across the country. While the crowds were calmed in Kenya and Putin has brought the Russian opposition movement increasingly to heel, these events show how political developments can expose companies operating in the country to serious risk. Future events may well hit those outside the country just as hard. When these governments leave office, what will be left behind them, and who and what will replace them?

Political risks, then, are not about to slow their rise in saliency. With international supply chains providing cheaper goods and outsourcing providing cheaper labor, firms are more and more exposed to risks in places on the other side of the world. Moreover, in the century of multipolarism, where billions of people across the world are expected to move into the middle classes and come into an income bracket that demands the import of high-quality foreign goods, the growth of a whole new swathe of export markets will bring these risks closer than ever to home.

WHY CARE ABOUT POLITICAL RISKS?

Recent developments have provided a stark reminder to organizations that political risks can affect their activities, objectives, and profitability. Crises such as the Eurozone negotiations, the debt ceiling debate in the United States, and the Arab Spring protests throughout North Africa and the Middle East took form rapidly and with little advance warning. Threats by the Iranian government to close the Straits of Hormuz have had a direct effect on oil prices. Other types of political risk—including state actions to promote state-owned companies, tapping into the cash flow of companies operating within national borders, and erecting trade barriers—have reemerged and pose significant problems to many companies.

Yet, while the management of financial, market, and other types of risk has become a paramount business consideration since the economic crisis of 2008, Accenture's 2011 Global Risk Management Study found that most companies do not measure—or manage—political

risk. Organizations tend either to accept these risks or to avoid opportunities altogether when they pose large political risks. The management of political risk, however, can be a competitive differentiator that enables companies to enter and navigate new markets and business environments.

The report concludes that the benefits include:

- Lower risk management costs through more rational hedging and insurance purchasing
- New revenue streams obtained through access to markets that would be too risky without risk management support
- Increased ability, confidence, and organizational buy-in for growth strategy in frontier markets
- Improved performance of existing business in emerging markets
- Loss mitigation through improved crisis management

Source: Accenture, *Managing Political Risk: Controlling Loss, Finding Opportunity*, 2012.

TERRORISM

Terrorism is, of course, technically a part of geopolitical risk, but such is its perceived impact on business that it is worth discussing separately. This sentiment is doubtless fueled by the tragic 9/11 attacks, which targeted not only government, but corporate interests. Al-Qaeda in particular understands the importance of economic targets, but terrorist groups have long sought to impact policy by targeting the corporate sector. The Provisional Irish Republican Army (PIRA) was particularly notorious in this regard, conducting a 25-year campaign in England, which killed 125 people and wounded over 2,000 more. The latter stages of this campaign saw several high-profile attacks on the financial sector in the UK, including the Baltic Exchange bombing of 1992, the Bishopsgate bomb of 1993, and the 1996 Docklands bombing. Further afield, the FARC in Colombia have also mounted attacks on economic targets (mainly oil pipelines) and have targeted business personnel as part of kidnap-for-ransom activities.

The 1993 Bishopsgate bomb was one of the main events to help build up the idea of business resilience, along with the jihadist attack that same year on the World Trade Center in New York City. This saw an attempt to topple the North Tower into the South Tower using a 1,300-lb

vehicle-borne improvised explosive device (VBIED). The attempt failed due to the vehicle not being able to park close enough to the support column it was intended to target; the homemade explosives used were also affected by the dampness, lowering the yield. The attack nonetheless still killed six people and wounded over a thousand more. The targeting of this center of economic and commercial power would of course be repeated in 2001 (see sidebar).

RICK RESCORLA

Cyril Richard "Rick" Rescorla was director of security for Morgan Stanley Dean Witter at the time of the 9/11 attacks. A colorful character, Rescorla had served in the British army as a paratrooper and intelligence specialist and then been active in Rhodesia before eventually joining the US military, serving with the 7th Cavalry Regiment, 1st Cavalry Division (Airmobile) at Ia Drang. He was described as "the best platoon leader I ever saw" by Maj. Gen. Hal Moore, who commanded at the battle and later cowrote the famous book, *We Were Soldiers Once…And Young*.

Rescorla joined what was then Dean Witter Reynolds in 1985, working at the firm's World Trade Center (WTC) offices in Manhattan. The 1988 bombing of Pan Am Flight 103 brought his attention to the potential terrorist threat to Western targets. In 1990, he therefore brought a friend who was a counterterrorism specialist to examine security at the World Trade Center. The key question asked was how he would target the building were he a terrorist—a classic example of red-teaming (see Chapter 13). The conclusion was that load-bearing columns were easily accessible via the parking garage, and this was highlighted in a report for the buildings' owners later that year.

As shown in 1993, this turned out to be a highly accurate assessment. Rescorla continued to advise his employer to move out of the building, which he considered—again accurately—to be a persistent target. However, the bank's lease on the property would not expire until 2006, and breaking this was too expensive. Instead, the firm agreed to other mitigation measures, including mandatory evacuation procedures that were taken very seriously indeed. Although this often brought Rescorla into conflict with senior executives, they too were expected to carry out the drills when the test alarm went off, being hauled off business calls or out of meetings in order to participate.

Although Rescorla was doubtless cursed by a number of people, especially when he deployed his stopwatch to explain why they weren't evacuating fast enough, this of course all paid off at 08:46 on September 11, 2001. When the first plane hit Tower 1—opposite Morgan Stanley's offices—Rescorla ignored the announcement to stay put and began ordering a mass evacuation of all employees. Notably, even visitors to the building who had come for a training class knew what to do, as they had also been exposed to a full safety briefing. Eventually, over 2,600 of the firm's employees were safely evacuated as a result of Rescorla's intelligence-led foresight, preparation, and planning—saving untold lives. Indeed, many were well on the way out of the building before their own tower was hit by the second plane.

In a further example of his leadership, Rescorla sang to the evacuees to maintain morale. Most tellingly of all, he kept returning to the tower once his own people were safe, in order to help others. He was last seen on the tenth floor, heading upwards, shortly before the building collapsed.

Although it might be easy with hindsight to castigate Morgan Stanley for not moving from the WTC site, the reality remains that risk must be balanced with cost. Mitigating the risk by giving Rescorla the top-level backing to implement effective and life-saving procedures ultimately worked, and this serves as a salient example of corporate security intelligence at work (Figure 2.1).

One of the other more shocking events in recent years was the November 26, 2008, attacks on Mumbai. A team of raiders came ashore and targeted multiple sites, including two luxury hotels. Business travelers were deliberately targeted. Although India is one of the states in the world most affected by terrorism, this has traditionally focused on government targets or the general Indian populace, rarely on foreigners, and certainly not on this scale. The incident therefore caused great concern, with many companies locking down all travel to India, passing up a great deal of business as a result.

Ultimately, terrorism is not a new tactic in any shape or form. However, increasing media coverage is making the impact of terrorism more acute. To be effective, the tactic has to result in publicity, and this is now easier than ever. Indeed, Ayman al-Zawahiri, leader of al-Qaeda, has proclaimed that the Internet is a sign from Allah that the group is on the right path,

Figure 2.1 Rick Rescorla's name at 9/11 Memorial.

since it allows jihadists to mobilize, recruit, and deliver their message more easily than ever before. Al-Qaeda has certainly been quick to grasp the opportunity offered, and although the shape of the global struggle continues to evolve, jihadist terrorism looks set to remain a feature of the corporate security operating environment for many years to come.

One of the more recent reminders of this was the In Amenas gas field attack in Algeria in January 2013. This site was operated by Sonatrach, Statoil, and BP, with the Algerian military responsible for providing perimeter security. The first official investigation into this incident was produced in September 2013 on behalf of Statoil. Although this steered clear of apportioning blame, it did highlight a need for much higher priority for security issues and more resources.

UNDERSTANDING GLOBAL JIHADISM

Global Jihadism is the predominant international terrorist threat, at present. Although the focus has long been on al-Qaeda, the rise of the Islamic State group (IS) in 2014 has recently lead to a schism in the global jihadist movement. This is highly dangerous, as the most powerful groups are now vying for credibility and support from the wider radicalized population. This also offers multiple avenues for radicalization, and numerous sponsors for plots, causing increasing levels of difficulty for intelligence agencies striving to contain the threat.

Despite the competition from IS, al-Qaeda remains the predominant international terrorist organization, although it is important to understand that it is more of a movement than a coherent group. Its aim is the liberation of al-Aqsa mosque in Jerusalem, which is the third holy place of Islam, and the restoration of a pan-Islamic *Khilafa* (Cailiphate). Al-Qaeda is to some extent also an apocalyptic cult, believing that these actions will bring about the end of days—believed by them to be the second best time to be a Muslim, beyond living in the days of the Prophet himself.

Ayman al-Zawahiri, the current leader of al-Qaeda, is more of a thinker than his predecessor and is less popular amongst jihadists. However he has always been the main strategician of the global movement, and although things have evolved since Osama Bin Laden's death in Operation Trident Spear, ultimately the course of the organization has not faltered.

Al-Qaeda's current structure is as follows:

- The **Core leadership** remains hidden predominantly in the tribal areas of Pakistan, where training facilities also still exist. This core sets the global agenda and coordinates between different parts of the movement. It sometimes has a role in attacks, although less frequently than hitherto due to US interdiction with drones and high level of interception of plots emanating from Pakistan.
- **Regional franchises** exist in a number of places. The most threatening at present is al-Qaeda in the Arabian Peninsula (AQAP). This group is based in Yemen and has attempted several strikes on the US homeland, mostly via aviation. It maintains a particularly anti-US focus and more aviation and maritime attacks are likely to emanate from AQAP. It poses an enduring threat to Saudi Arabia.
- Al-Qaeda's stake in the **Syrian civil war** is represented by a number of groups, but mainly the al-Nusra front. However, the credibility of this grouping is dropping due to the rise of Islamic State in this region.
- The latest addition is **al-Qaeda in South Asia**. This group launched an abortive attack on the Pakistani Navy in September 2014, but has achieved little more as yet; it remains something of an unknown quantity.

- Al-Qaeda also has a strong franchise in Northwest Africa, **al-Qaeda in the Islamic Maghreb (AQIM)**. This has a distinct anti-French focus, given its colonial heritage.
- **Regional allies and affiliated groups** include movements such as **Jemaah Islamiyyah (JI)** in south-east Asia; Kashmiri focused groups operating out of Pakistan, such as **Lashkar-e-Taiba (LeT)**; and **Ansaru** in West Africa.
- Finally, al-Qaeda seeks to **inspire individuals or self-motivated cells** in other countries, especially in the US, UK and Europe. As mentioned above, formal plots have become more difficult to launch and so al-Qaeda increasingly relies on "open source jihad," under which both the intent and capability of would-be attackers is enhanced through the internet.

In summary, al-Qaeda seeks to be a vanguard—setting the way for others to follow. Their key tenet is to do as they believe they should do, and not heed criticism. It has a long-term strategy gradually to mobilize the mass of Muslims in order to liberate al-Aqsa mosque, restore the *khilafa* and eventually bring about the end of days. The seeming failure of Islamist governments is taken by the movement to be an encouraging sign that their way—the use of force—is the "right" way. This means that the threat is not receding, and the Arab Spring has greatly increased the opportunities open to the group.

However, many jihadists consider that al-Qaeda has failed to produce anything meaningful for a number of years, or have other doubts about the group's ambitions or legitimacy. The rise of IS has therefore been very attractive, not least those who have travelled to fight in Syria. The group's sudden successes in Syria and Iraq, coupled with the symbolically vital announcement of the caliphate, has made it a lodestone for a new wave of jihadists. The group has a notably more violent trend than core al-Qaeda, based in part on its antecedent, al-Qaeda in Iraq, founded by the late and unlamented Abu Musab al-Zarqawi. This was always a controversial entity, but since 2012 it has become more practical, forging alliances of convenience that overcome the constructs of religious dogma. This includes partnering with Sufis and even selling oil (its chief revenue driver) to its adversaries in the Syrian government. The leadership seems genuinely to be trying to establish a lasting Sunni Arab *khilafa* in *al-Shams*

(Lebanon, Syria, Israel, Jordan and Iraq), an area of historical and prophetic significance.

The growth of Islamic State has been accompanied by a very effective PR campaign from the group, which has driven the gradual emergence of more and more regional allies. These are more or less completely operationally separate from IS, but show the fracturing of the jihadist movement away from al-Qaeda core. The latest additions include groups in Pakistan, Afghanistan, Libya, Algeria and North Sinai, with more expected to follow, including in West Africa and South-East Asia. An extension into Saudi Arabia, Yemen and eventually Jordan also seems inevitable.

The Paris attacks show the considerable danger from the fracturing of the jihadist movement (combined with the damaging effects of intelligence released by former NSA operative Edward Snowden). The three people involved in operations were motivated and supported separately by AQAP and IS. The burgeoning networks are complicating the job of the intelligence community, and increasing the amount of radicalizing material that is available. They are also increasing the sources of funds. While most threat actors will continue to focus on "valid" or "legitimate" targets such as the military and security forces, not least as the battle for credibility and legitimacy continues within their target audiences, the risk of more or less freelance actors taking even simple steps to carry out attacks means a huge range of threats exist. At the simplest end, these include attacks using cars or basic weapons in crowded places, but—as Paris shows us—more advanced plots using sophisticated tactics remain possible. The flow of fighters back from theatres of jihad in fact makes such operations more and more likely, posing an ongoing threat to corporate operations in many regions of the world.

In the international arena, key terrorism threats to companies include:

- Kidnapping of employees, including locally employed personnel (often overlooked but sometimes a more significant terrorist target than Westerners, if a struggle is more local than international in focus)
- Targeting of physical assets
- Mass casualty attacks on crowded places, often using multiple improvised explosive devices

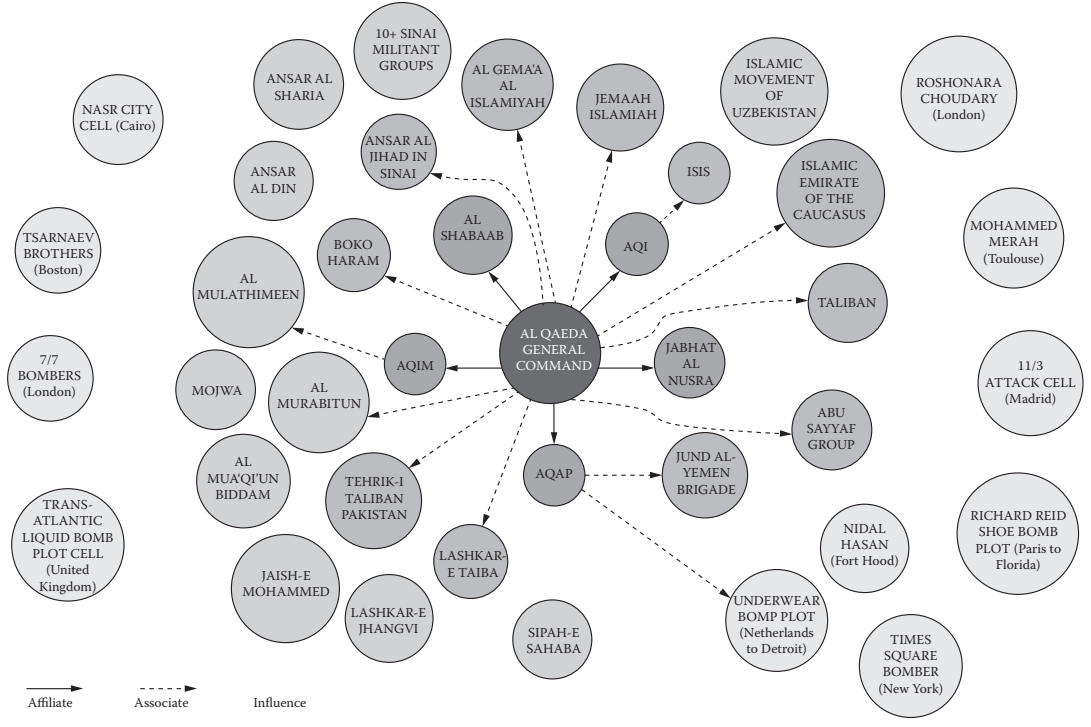

Figure 2.2 The structure of the global jihadist movement in early 2014; since this was drafted, ISIS has evolved considerably and has *de facto* eclipsed al-Qaeda Central as the main threat actor and inspiration for others. This underscores the rapidly changing nature of the terrorist threat. (From Noman Benotman and Jonathan Russell, "A New Index to Assess the Effectiveness of Al Qaeda." Courtesy of the Quilliam Foundation.)

- Interdiction to supply chains
- Interdiction to transport (e.g., the Maoists in many rural areas of India)

In addition to international terrorism, domestic terrorist activity is also a concern. Again, this is hardly a new phenomenon, although the attack on the Boston Marathon has served to refocus attention on the "lone wolf" angle. Again, many previous incidents have focused on government assets, for example the Oklahoma City bombing of 1995 or the shooting of several CIA employees waiting at a traffic light near their headquarters in Langley, Virginia, in 1993. Deliberate targeting of corporate interests has generally occurred as a result of single-issue campaigns, and this serves as notice of a potential threat that is likely to grow due to socioeconomic and geographic factors.

Terrorism is, then, something of a fact of life. However, in general, targets are chosen because of their high media impact and because they are "soft." The In Amenas report particularly highlighted the insider threat, and reconnaissance is a key part of target selection for most groups. An intelligence-led approach is therefore vital when dealing with a terrorist threat, as comparatively simple measures, including *synergistic controls* (see Chapter 13) can greatly help to reduce exposure. Moreover, fine understanding of the nature of the threat can entail the ability to continue doing business safely in markets that others might deem to be too high risk.

CYBER ISSUES

Just as the world experienced an Industrial Revolution in the late 1700s and early 1800s, the last twenty years have seen a revolution in information. In the same way as the Industrial Revolution drove dramatic changes to productivity and economic growth, the advent of the Internet has radically improved the speed of global communication and has exponentially increased the amount of information we can access. This revolution has arguably touched every aspect of human endeavor. Culture, art, science, sport, and business have all been influenced by the opportunities and efficiencies offered by the Internet and its associated technology, bringing a range of far-reaching benefits to humanity.

As with most revolutions throughout history, not every aspect of the information revolution has been positive. The speed of communication

and the availability of information have been exploited by a range of actors seeking to further the cause of their country, to steal, or to undermine the existing societal structures in pursuit of political change. States and their supporters conduct cyber attacks and cyber espionage, major criminal organizations increasingly conduct operations online, and political activists seek to cause disruption in cyberspace.

Along with the development of the information revolution, we have seen the parallel development of a new field in security, commonly referred to as *cyber security*. As the information revolution can be argued to touch every aspect of human endeavor, so too do the threats and risks of the cyber security landscape.

In systemic terms, the cyber security landscape is more comparable to international security than the internal security of a state. Just as the international environment is composed of disparate actors striving for supremacy without an effective policing structure, the wide reach, complexity, and anonymity of the cyber environment make effective policing highly challenging. This puts the burden of security far more on individuals and businesses than we see in the physical world. Effective cyber security starts with this realization.

The range of cyber threats to target businesses can be organized into three main categories, namely, State Level, Cyber Crime, and Cyber Activism. These are illustrated fully in Table 2.1.

Table 2.1 Cyber Threat Categorization

Category	Type	Threats to business
State level	Cyber attacks	Potentially targeting physical infrastructure, data storage, and cyber operations
	Cyber espionage	Potentially targeting intellectual property across a wide range of industries
Cyber crime	Theft	Cyber criminals target banking details, cargo shipments, and other financial transactions
	Fraud	Common scams targeting businesses include identity theft and financial misrepresentation to businesses
Cyber activism	Attacks	Includes website defacement and theft of data from businesses
	Organization	Developing and coordinating activist campaigns targeting businesses

State-Level Threats

Just as nation states dominate the physical security environment, the economic and human resources at their disposal place them at the apex of cyber security threats. These threats fall into two categories:

- *Cyber attacks*: Cyber attacks can be defined as acts carried out through cyberspace that have the intent to damage or destroy physical or cyber assets. One such example of a physical cyber attack was the 2010 Stuxnet attacks carried out against the Iranian uranium-enrichment facility at Natanz. This attack involved the injection of malware onto the facility's network that was specifically designed to target the control systems of uranium centrifuges, manipulating these in such a way as to physically damage them. Cyber attacks can also be carried out against other cyber assets such as networks and individual devices, with the intent of disrupting their operation or destroying data.
- *Cyber espionage*: Espionage is an ancient art form, practiced for as long as humanity has been engaged in organized conflict. Cyber espionage is a development of this field and can be defined as an act carried out through cyberspace to gain access to privileged information without consent. Cyber espionage is not exclusively linked to state actors, but these overwhelmingly dominate the environment. Much recent attention among security researchers has focused on the activities of the People's Republic of China and their alleged targeting of foreign governments and private firms across a wide range of industries. While China may dominate the headlines, other large and mid-level powers also maintain active cyber espionage programs.

Cyber Crime

Just as legitimate businesses do, criminals are motivated to maximize their financial returns while at the same time minimizing risk. This has driven innovation so that the criminal world now keeps up with technical and societal developments. The information revolution is no different, and criminals have embraced the opportunities to move against a far broader range of targets while utilizing the anonymity the Internet can bring. Cyber crime can be organized into two main categories:

- *Theft*: The Internet facilitates numerous forms of communication and interactivity that are entirely removed from direct personal

contact. In a traditional banking environment, a customer may attend a branch and physically sign a withdrawal slip in front of a cashier. In online banking, all that is generally required is an individual's login information and potentially a two-factor authentication code. Cyber criminals have utilized a range of malware to circumvent these controls, in one instance stealing an estimated $47 million from European bank accounts in late 2012.

- *Fraud*: Cyber fraud involves the active misrepresentation of information in the cyber environment with the intent of making a financial gain. This includes advanced fee fraud, often conducted from West African countries and involving the nonexistent estates of deceased regional heads of state. Increasingly, sophisticated fraud practitioners are targeting businesses in the pursuit of ever larger payoffs.

Cyber Activism

As with the *state* and *cyber* crime categories discussed here, the world of social and political *activism* has also been quick to leverage the cyber landscape to organize and promote their causes. At the same time, we have also seen a rise in so-called hacktivists, groups of hackers who either seek to destabilize the established order or who seek to initiate social or political change.

The most well known of these is Anonymous, originally an almost nihilistic group of hackers who have evolved over time to specifically pursue activist causes and which has established a sizeable presence in the physical activist community. Hacktivists are renowned for targeting corporations, defacing websites, and stealing data. While several key hacktivists have been arrested and convicted in recent years, organizations such as Anonymous retain a significant capacity and intent.

A New Paradigm

Cyber security presents a unique challenge to businesses. Although still relatively unlikely, state actors may launch cyber attacks against businesses, while state-driven cyber espionage is alarmingly widespread in the corporate sector. Criminals are increasingly turning toward cyber operations, and cyber activists are seeking to organize as well as operate in cyberspace.

In light of the difficulties with policing the Internet, businesses must adopt a far greater responsibility for their own cyber security than with their physical security. In this sense, they must operate in a relatively new paradigm with a rapidly evolving architecture and threat environment. However, as discussed in Chapters 7 and 13 in this book, the cyber landscape presents opportunities as well as threats.

CONVENTIONAL ESPIONAGE AND THE "INSIDER THREAT"

Having considered the threat posed to a firm's intellectual property by external actors, often in the form of malware-based espionage, it is now worth considering the other side of the counterintelligence coin in the form of the insider threat. Carnegie Mellon University's Computer Emergency Response Team (CERT) defines an insider threat as "a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems." This therefore includes the traditional espionage agent, whether for a foreign power or a hostile company, as well as, increasingly, the ethical whistle blower (viewed in some security circles as "the new ideological defector").

Insider threats have undoubtedly resulted in some of the most spectacular data breaches in the history of intelligence. While working for the RAND Corporation as an analyst in 1971, Daniel Ellsberg released what came to be known as the Pentagon Papers, a series of classified documents that revealed successive administrations' deliberate deception of both Congress and the public over the United States' involvement in Vietnam. While Ellsberg's whistle-blowing represented an almost unique alignment of opportunity (in terms of the exceptional access provided through his seniority) and motive (in the form of his increasingly ideological opposition to the war), more recent examples underline the shift to a different paradigm. Both former PFC Bradley Manning's 2008 release of thousands of confidential US diplomatic cables to Wikileaks and Edward Snowden's revelations about NSA surveillance programs in 2013 highlighted the exponential growth in access to sensitive information, especially when considered in the context of institutions that place a premium

on information security. This development is reinforced by recent revelations in mainstream media that nearly 5 million people in the United States currently hold some level of security clearance, with 1.4 million of those possessing top-secret clearance or above.

Indeed, it is this notion of increased access for all that has enhanced the significance of the insider threat in the contemporary corporate security environment (a theme that we will also come back to when considering "need to know" versus operational security discussed in Chapter 10). While the transition from analog to digital information storage and the associated ability to effortlessly replicate data was momentous in terms of its implications for information security, the subsequent shift from a model of data held by servers protected by a clearly defined perimeter to the current trend of freely accessible data, bring your own device (BOYD) policies, and systems of cloud computing has exacerbated this effect and ensured the enduring relevance of the insider threat. This development is only likely to be further entrenched and expanded as the convenience and other benefits afforded by such modern methods continues to outweigh and outpace the accompanying security considerations.

Despite this historic prevalence and increasing relevance as a threat vector for business, the significance of the threat posed by such insiders has consistently been underplayed, a tendency that can be attributed to several factors. Firstly, media and public interest in and representation of this vector pale in insignificance compared to more dramatic and romantic narratives of daring espionage operations and sophisticated hackers breaking systems from the outside. Secondly, due to the insider's familiarity with the internal security environment of a particular firm, breaches of this nature are often harder to detect, while the difficulty in quantifying the volume and value of material accessed further obscures the significance of this issue. Thirdly, while it is already difficult, if not impossible, for a firm to develop a solution that completely mitigates the threat from external parties, the search for a solution becomes significantly more problematic when the threat is located within a firm's security perimeter. Though some countermeasures are possible, such as prerecruitment screening of employees to identify potential threats and compartmentalization of information to limit unwarranted access, there is certainly no silver bullet to nullify the insider threat. The difficulty in reaching a solution to balance security and accessibility, as well as the implications for firms to adopt more restrictive measures, provide further disincentives toward discussion of this issue.

Notable examples can be used to illustrate the importance of the insider threat in the modern business environment. In 2011, the Massachusetts-based energy firm American Superconductor (AMSC) suffered severe financial losses after a deal with Chinese wind-turbine manufacturer Sinovel collapsed. The breakdown in negotiations followed the transfer of a key piece of power-regulating software by Dejan Karabasevic, a disgruntled engineer. When combined with the prospect for personal financial gain, the existence of employee dissatisfaction in the workplace can provide a compelling motive for the transfer of sensitive information to a third party. Karabasevic, who had been demoted shortly before his departure from AMSC, later took up a lucrative contract with the Chinese firm in an apparent attempt to obscure the nature of his contribution. The leak cost the US firm an estimated $800 million, in addition to the loss of 500 jobs from the failed project.

Though the case of AMSC provides a succinct example of the danger of the insider threat, it is somewhat of an exception, as the losses that result from an insider breach are generally more ambiguous and less quantifiable. This is especially the case where the theft took place over a protracted period of time, as was the case with Dongfan "Greg" Chung's theft of sensitive information from Rockwell International and Boeing over a thirty-year period. Chung was discovered with 300,000 pages of sensitive information at his California home, covering a variety of aerospace and defense projects. Crucially, despite this massive theft of data, authorities were unable to prove that the engineer had been able to transfer the information to the Chinese intelligence apparatus, let alone estimate the value of any information that was delivered over this considerable period. It is difficult to underestimate the impact of such known unknowns that contribute to the pervasive atmosphere of doubt associated with the insider threat to the corporate security environment—and, again, few cases are publicized. Despite the focus on *cyber* as an issue, the threat from human penetration of organizations therefore remains very real, with persuasion and coercion being used by adversaries seeking to gain a decisional or technical advantage.

SINGLE-ISSUE ACTIVISM AND POLITICAL VIOLENCE

Single-issue activism and political violence can have considerable effects on an organization's reputation, its employees, and its continuity, regardless of whether it is the target or has been collaterally affected by some

other action. Moreover, the potential for an organization or business to be affected is ever growing. With the emergence of social media, single-issue campaigns are now regularly established and can often gain traction quickly, with little warning. There is also an emergence of the belief among activists that all liberation struggles—particularly those against the state and corporations—are actually parts of one overarching struggle and should be united, making networks wider and campaigns stronger. Lately, secondary or tertiary targeting has become a common tactic in campaigning when aims are unachievable through pressure on the primary target alone; under this tactic, suppliers, financial backers, and clients of target companies become the focus of campaigns. Therefore, it remains ever important for organizations to keep abreast of current issues and of how these could affect their business.

Each of these key themes is important, and so we will review each in turn.

The Move toward All Liberation Struggles Being "As One"

Traditionally, single-issue activists and groups based most of their focus and campaigning on one essential policy area or idea. While single-issue campaigns still exist independently, since the mid-2000s, there has been a notable shift toward all liberation struggles being seen as part of the same overarching effort. The very term *single issue* is therefore now something of a misnomer, with activists often turning out to support a number of issues, largely out of "solidarity"—an ever-more-important concept.

In this regard, the Occupy Movement has been a distinct enabler. Despite a meteoric rise from September–December 2010, this movement is now more or less totally physically defunct in most areas (although the symbology lives on). However, the information network created by so many activists from various causes coming together (largely on social media) has created a much larger support base for actions by members. It has also served to help publicize events, spread knowledge of tactics, and allow for the effective coordination of potential attendees. This has resulted in notably increased interrelationships between groups and causes.

A good strategic example is provided by the recent growth of environmentalism, the broad philosophy, ideology, and social movement that advocates the preservation, restoration, and improvement of the natural environment. The preservation and restoration aspects of the movement often incorporate numerous campaigns that focus on a long list of issues, including the use of sustainable energy, recycling, localism,

anticonsumerism (often tying in with anticapitalism), the merits of organic produce as opposed to that treated with pesticides and chemicals, and production of genetically modified (GM) foods. Fracking, or hydraulic fracturing to release hydrocarbon deposits, is also a particularly hot issue at present. The balancing side of the movement, which advocates that humans and the environment should be given equal respect, has given rise to animal rights movements such as campaigns against farming and vivisection and the advocating of vegetarianism and veganism. Furthermore, the recognition of humanity in the ecosystem, and the balance between different species, whether human or nonhuman, draws heavily on human rights, with involvement in antiwar campaigns, socialism, and women's and minority rights. While these appear to be separate areas, nowadays activists are more likely to brand themselves as environmentalists and so be willing to turn out to support any and all of these causes.

Secondary Targeting of Customers, Suppliers, and Shareholders

Activist groups seeking to bring about change are increasingly targeting their primary target's customers, suppliers, and shareholders in order to achieve their main campaign goals. This tactic has been highly successful, offering an exponential range of targets. Many of these secondary targets are not prepared for the controversy that such actions can bring, making them highly vulnerable; this in turn leads to increasing isolation and pressure on the intended main target. As a result, secondary and even tertiary targeting continues to gather in both pace and popularity. At the time of writing, ongoing examples include the targeting of KFC due to it being a customer of a Greenpeace target; campaigns against Barclays Bank as an alleged supplier of finance to arms companies; and the targeting of Astra Zeneca's suppliers (including financial sponsors) in relation to its reported patronage of Huntingdon Life Sciences. In all these cases, the awareness of the main campaign can result in a number of separate groups targeting the entity concerned, with many campaigns also drawing significant hacktivist activity, as previously described.

Internationalization of Single-Issue Campaigns

Numerous factors such as the creation of the European Union, greater globalization, developments in communications, and an increase in physical mobilization have given rise to a vast uptick in international university study, work, and travel, all of which have contributed to the

internationalization of single-issue politics and political activism. It is now common for activist groups to have branches in countries across the world and regularly conduct international days of coordinated protests against a particular target or for a certain cause. Moreover, due to greater interdependency, issues in one area of the world often now lead to protest actions in another. For example, disputes over agricultural land in Palestine are currently leading to protests at Marks and Spencer stores in the UK and other companies internationally. This spread is increasing the awareness and effectiveness of such campaigns, driving higher turnout and greater levels of public interest, while also offering a larger sense of community and solidarity to those involved.

Political Extremism

Given ongoing societal changes, the means by which political extremes are voiced are ever growing and are frequently expressed in ways that can affect corporations. For instance, of great concern are far-left and anarchist groups who particularly target business premises that they regard as major contributors to a failing capitalist system. Since the collapse of Lehman Brothers in 2008 triggering the global financial crisis, the UK, United States, Europe, and elsewhere have seen tightening economies, austerity measures, and colossal cuts on public spending, all of which contribute to the anarchist ideology and cause. In the most extreme cases, left-wing and anarchist groups voice their grievances through violence. In this regard, a notable increase was seen in the years following the start of the financial crisis; according to reports by Europol, there were twenty-eight left-wing and anarchist terrorist attacks in Europe during 2008, forty in 2009, and forty-five in 2010. Naturally, nonviolent action stemming from left-wing and anarchist entities is also ever increasing, with protests, civil disobedience, and online campaigns often carried out against corporate (as well as government) targets.

Religious–political extremism also continues to be a major concern for organizations globally. While this could be with regard to demonstrations being held near offices, inadvertently affecting business operations, on some occasions such extremism can directly impact a business or its employees. For example, clothing stores have been targeted by Islamists seeking to instill Sharia law on the basis that they consider them to immodestly display merchandise. On more sinister occasions, employees of certain organizations have been threatened for not wearing hair or face coverings. Such Islamist extremism—in addition to the events of

September 11, 2001, July 7, 2005, and more recently the US Boston Bombings and UK Woolwich attacks in 2013—also further fuels right-wing extremist activity, which can have equally as much impact on corporations globally, both directly and indirectly.

Use of Social Media in Single-Issue Protest and Political Activism

As mentioned previously, activists recognize the utility of social media as a communications tool both to recruit people to causes and publicize physical gatherings and protests. This has led to increased networking between groups, and campaigners' communications now allow for large-scale, coordinated action, often at short notice (although there has been a converse shortening of most protestors' attention span over issues, with many routinely looking for the next new thing). Moreover, activist groups now capitalize on technology to assist in civil disobedience during protests, as was seen by the invention of the antipolice smartphone app Sukey in the UK. Nevertheless, the use of technology to further their causes has also meant a shift toward campaigns being orchestrated and organized through open-source channels. While misdirection is not unknown, and veiled speech is sometimes used, this does offer an advantage in terms of spotting potential actions and examining trends for guidance in developing indicators and warnings.

ORGANIZED CRIME

Organized crime (known as *serious organized crime* in the UK), both national and cross border, is better understood as a mechanism fueled by much the same factors as those that expand trade and development, communication, infrastructure, and health. This is evident at any level of crime, from pickpocketing to counterfeiting, shoplifting to money laundering. Where there is a demand, there is traditionally a supply, and criminal syndicates worldwide continue to find loopholes to raise profit via illegal means. Thus the term *organized crime* encompasses a wide range of national and transnational illegal activity that jeopardizes the economic and political stability of societies, in addition to posing a direct threat to life and development.

While law enforcement agencies—local, national, and international—continue to increase and improve their efforts to protect citizens against the ever-evolving nature of serious organized crime, there is also an increasing need for corporations to take a proactive, intelligence-led approach to protect their operations, assets, and integrity. The aim of this chapter is therefore to review the challenges that serious organized crime poses to the growth, development, and reputation of corporations and to examine the role of an effective intelligence-led approach to detecting, preventing, combating, and mitigating such activities.

The Wide Reach of Serious Organized Crime

In its broadest form, serious organized crime refers to a number of illicit activities that are carried out by a group or groups of individuals on a continuing basis. In essence, these are criminal organizations that work together for the duration of one or more criminal activities. The Serious Organized Crime Agency (SOCA) in the UK follows the government's Organized Crime Strategy "Local to Global" definition of organized crime as

> Individuals, normally working with others, with the capability to commit serious crime on a continuing basis, which includes elements of planning, control and coordination, and benefits those involved. The motivation is often, but not always, financial gain.

Much as in any legitimate organization, criminal organizations often involve a criminal syndicate or a core group of syndicates at the top of the hierarchy. Similarly, further down the ladder, there may be subordinates, specialists, associates, and runners, depending on their experience and skills.

In a further similarity to legitimate business environments, criminal networks engage in a wide range of illegal activity across a wide range of sectors. Activities include

- Counterfeiting/Intellectual property crime
- Corruption
- Illegal trade
- Theft of commodities and assets
- Kidnap and extortion
- Money laundering

Threats to Corporate Security

A particular threat posed by the illegal activities of serious organized crime groups is that their actions may go unnoticed for long periods of time, with the attendant potential for catastrophic consequences for businesses. These consequences may be measured in terms of financial loss, reputational damage, or even direct harm to people and property. However, it is important to note that such activity may not be explicitly illegal. Working under the cover of legal operations, money laundering, bribes, and fraud remain at the core of illegal transactions. In addition, such activity may be further connected to—or even fund—other types of serious organized crime, including smuggling of drugs and people, the illegal arms trade, and terrorism, thereby extending the impact of its consequences from the business itself to the development, operations, and even lives of others.

Intellectual property theft and counterfeiting: No brand or label has been able to establish complete immunity from intellectual property theft or counterfeiting. This is evident across flea markets and Internet sites alike, and the news continues to report seizures of counterfeit video games, clothing, and pharmaceuticals. Viagra has arguably shown to be one of the most popular on the counterfeit pharmaceutical market due to its high retail price, while Apple has heightened its manufacturing security following an increase of counterfeit iPhones and other merchandise on the black market.

Corruption: Corruption is perhaps most evident in emerging or unstable economies where transparency is limited or absent altogether. A recent example was illustrated by the IKEA corruption case in Russia, which resulted in the dismissal of the company's two executive managers in the country after allegations of bribery. The scandal emerged after it became apparent that the executives paid off Russian insurance and energy companies to retroactively approve all electrical installations at IKEA's facility in St. Petersburg. While these actions were arguably not directly for the executives' financial gain, their actions did cause direct damage to the integrity of the company.

Theft of commodities and assets and illegal trade: The theft of commodities and assets, e.g., theft of metal from building sites or theft of cargo in transit, remains as an active threat faced by a wide range of industries. With wide-reaching and well-established criminal networks, organized groups are able to move commodities

nationally and across borders, avoiding detection much in the same way as those operating illegal drugs or the weapons trade, or even in tangential connection with these operations.

Kidnap and extortion: Kidnap and extortion may also be a part of the wider organized criminal tactics in attempts to coerce, blackmail, or threaten corporations and/or employees into meeting demands, whether financial (in the form of ransoms), regulatory (forcing a corporation to work in a certain way), or physical (handing over assets, operational capability, or information).

Money laundering: Finally, what is considered one of the largest money-laundering cases of the twentieth century illustrates the wide extent of illicit activities that corporations may face. The Bank of Credit and Commerce International (BCCI) was founded in 1972 by a Pakistani financier and quickly established an operating capability of over 400 locations worldwide. Its rapid growth—ranking as the seventh largest private bank in the world by assets at its peak—attracted suspicion from financial regulators. Although BCCI contended that its growth was fueled by large deposits from oil-rich states and developing nations, investigations revealed vast amounts of fraud and money-laundering activities that supported the drug trade and corruption. In addition, it has been alleged that the CIA used the bank to fund the Afghan mujahedeen during the war with the Soviet Union in the 1980s. Following substantial reputational and financial damage, the bank shut down in 1991.

EMERGING THREATS—WHAT'S NEXT?

Horizon scanning is a critical activity for corporate security intelligence professionals, as we will discuss in Chapters 5, 6 and 13. The ability to forecast how threats may evolve is important to enable early mitigation. To give just one minor example, predicting the rise of viruses and other attacks that exploit mobile technology has enabled several firms to build in risk controls as part of their IT policy from day one, whereas others are now scrambling to work out how to deal with this problem. It is therefore apposite for us to consider the question as to how threats will evolve.

In this regard, it is perhaps worth discussing anticipated global developments to 2030. By then, median estimates of population expansion place the total world population at around eight billion. Falling fertility rates offer the prospect of an aging population, although the effects of this

will be concentrated mainly in Europe and Japan. Emerging economies should see consistent growth, albeit at a potentially slightly slower rate than that seen over the past decade, and potentially over a billion people could be set to join the global middle class during this period. China and India in particular should continue to see notable growth. Although both countries face a number of hurdles, estimates suggest around 50% of global middle class demand could be driven by these two countries by 2050, significantly shifting markets from the United States and Europe.

The rise of emerging powers (China in particular) is expected to play into an increasingly multipolar world with no clear hegemonic power, a trend that may be exacerbated by a current American reluctance to commit troops to combat operations after the experiences of Iraq and Afghanistan. The United States will, however, remain predominant over this period in security terms, although the military capability gap will continue to close. Strong performance from China and India is expected to benefit key trading partners, although the rise of these new powers may present new diplomatic problems over issues that have hitherto remained dormant, such as territorial issues in the East China Sea and around the Spratly Islands.

Technological development is likely to continue at the steady pace seen in previous decades. While breakthrough technologies are possible, and surprises are certain, changes will generally be made incrementally. In health technology, steady breakthroughs and improvements should prolong the average life span, although an international pandemic remains possible, and the effect of this may be driven up by increasing global mobility and cramped living conditions. Social media and communication technologies are expected to continue a steady trend of growth, leading to more individual empowerment, although the current debate over governance of the Internet and privacy laws leaves the eventual impact of this information expansion quite uncertain. In due course, a trend toward increasing policing of the Internet seems likely, but this will need to be based on global consensus. Regardless, the cyber angle will drive more and more aspects of conflict.

Expansion and availability of technology, while empowering billions, is expected to impact threats from extremists and allow closely knit groups (whether religious or ideological) to exist in geographically distant locations. We expect Internet access to continue to rise as middle classes grow globally and the cost of the basic technology falls in comparison. More education is likely to be provided online, and this may lead to a diversification of sources, differentiating the disparity between online

information and online knowledge. Information will also become more readily accessible in a number of languages, although the way that this develops locally will depend upon legislative reactions to the Internet. Cyber security, already a significant threat, will grow directly in relation to the growth of communication and IT, with criminals known to be early adopters of new technology. This will present new challenges in policing and in security over time, and it is likely to influence military and defense doctrine in a way far greater than the initial attempts we are seeing today.

Energy supply will remain crucial, although how the various markets will play out still remains uncertain. The most likely models show that shale gas is expected to give the United States independence from foreign imports and potentially allow the country to export gas once again in the next decade. In contrast, European countries are expected to become more gas dependent over the period (with individual exceptions expected). The growth of China and India means that we expect to see increasing amounts of oil and gas transiting eastward, which may help to prop up prices in the face of reduced demand in the West and will give resource exporters a market choice, thereby reducing the reliance on Western demand. Indeed, by 2025, the amount of hydrocarbon products heading from the Persian Gulf to US markets is expected to be a tiny fraction of the volumes seen at the time of this writing.

Competition over resources may be the defining feature of the middle of the century. Climate change and population expansion will put increasing pressure on water sources, with estimates indicating a potential 40% increase in demand. This suggests an increasing need for a number of nations to manage freshwater resources more efficiently, particularly when shared sources are at stake. Freshwater supply is likely to become more strategically significant and may be a spur for disputes between upstream and downstream nations. Moreover, the need for desalination may help drive a strong expansion in nuclear power. Global food supply is likely to be subject to similar strains, with up to a 35% increase in demand possible, although potential steps forward in technology—including genetic modification—may help to mitigate impacts. Extreme weather events are likely to become more frequent, and the impact of natural disasters will also be greater due to increased building in flood zones and fault areas, coupled with increased population density and dependence on just-in-time manufacturing strategies.

Against this background, there are a number of potential threats and hazards: nuclear proliferation, an increasingly complex cyber environment, increased chances of state conflict, more likelihood of population

unrest, and a rise in movements related to environmental issues—some possibly espousing violence as a means to bring about change—seem more likely. Jihadist issues are also unlikely to recede, and more and more threat actors are likely to embrace asymmetric tactics. Many may even be supported by state sponsors engaging in proxy conflict, a situation that we are already seeing in the Middle East at present.

CONCLUSION: A COMPLEX AND MULTIFACETED WORLD

The range of potential threats facing a company can be overwhelming, and their impact can be high. Even companies that have not traditionally been exposed to more than the most rudimentary of security risks are now exposed to events thousands of miles away, which can disrupt supply chains and highlight dependencies that no one was previously aware of. Threats are networked and are often driven by interrelated issues. Given all of this, and the clear impossibility of forming a total barrier around the business (as may once have been the case), the vital role of intelligence in supporting an agile, dynamic, and efficient security function is obvious.

3

Legal Drivers for Corporate Security Intelligence

> All employers have a general duty to provide their employees with "a workplace free from recognized hazards likely to cause death or serious physical harm."
>
> **OSHA**

CHAPTER OBJECTIVES

1. To understand that both *push* (why you must) and *pull* (why you should) factors drive the requirement for corporate security intelligence.
2. To outline the main legislative and ethical imperatives that apply to corporate intelligence and risk management.
3. To illustrate how these imperatives apply in different jurisdictions (with special focus on the United States, UK, and Europe).

INTRODUCTION

Chapter 1 outlined some of the benefits of corporate security intelligence as a function, and why more and more organizations are building this capability. However, one of the greatest challenges encountered by chief

security officers (CSOs) is the need to demonstrate clearly why the function is of benefit. Ultimately, the service is to some extent intangible, so spending on beefing it up can look like spending more money on overhead. This adds to the common perception that security as a function is, in itself, purely a cost to the organization—something that CSOs have to fight every day. The question most commonly asked is therefore how to go about positioning and selling the security intelligence function within the business. This includes providing initial business cases and support to proposals, as well as then helping convince internal customers to use and support the service once funding has been achieved. The latter is sometimes a particularly long-winded process, although the good news is that usually once people see what intelligence can offer them, they embrace it heartily. Of course this then brings its own challenges—how not to oversell a service to the extent that demand outstrips supply and overwhelms the available resources.

Rolling out a service is thus quite a challenge, and so we address how to build and implement a full business and implementation plan in more detail in Chapter 12. For now, though, it's worth understanding the main factors at play when trying to build the argument as to why the service is required at all. For the purpose of analysis, we divide these into two areas:

- *Push* factors: These are things that force organizations toward having a security intelligence function. This includes legislation over such things as corporate manslaughter, duty of care, negligent failure to plan, and countering corruption (with both the Foreign US Corrupt Practices Act and the UK Bribery Act causing increasing concern over how to conduct operations overseas). Regulatory factors for some industries (or jurisdictions) also mandate minimum standards for business continuity and crisis management.
- *Pull* factors: The things about having a security intelligence function that help and benefit the business. This includes financial aspects as well as ethical considerations above and beyond those considered by legislative pressure.

Both of these aspects are important. Of course, executives initially tend to focus on what they *have* to do, given the general perception of security as being in essence a cost. Full consideration of the factors in play shows that actually it's what intelligence offers beyond the base legal requirements that is more beneficial, in the long run. However, it usually takes time, examples, and experience for people to fully realize this.

The general advice is therefore to consider all of the factors discussed in this book when planning to position a function, thereby building a case that is specific to the business, executives, and jurisdictions concerned. The discussion that follows is, therefore, broad ranging but offers at least a starting point for development of a specific set of benefits.

This chapter covers the more detailed factor—the legal angles and other legislative factors that drive reasons why an organization *must* have corporate security intelligence. We will then address the *pull* factors in Chapter 4.

The key issues we will discuss fall into two main areas, as follows:

- The employer's duty of care, corporate manslaughter, and negligence
- Corporate responsibility, regulatory compliance, ethics, and sanctions

Overall, these topics are worthy of a book in themselves and are of course extremely complex. What follows is therefore necessarily in depth, but within organizations, advice should still be sought from the in-house legal team; this is also advisable to help in understanding potential constraints to operations.

Protecting the Heath, Safety, and Security of Employees: An Employer's Duty of Care

Inherent in the relationship between employer and employee is the employer's *duty of care* for employees' health, safety, and security. The duty of care applies in a wide range of instances, and extends beyond the typical workplace environment. For example, the duty applies to employees and dependents when they are on business trips or international assignment, when they work from home, and may even extend to contractors and subcontractors. The legal concept of duty of care presumes that individuals and organizations have legal obligations to act toward others and the public in a prudent and cautious manner to avoid the risk of reasonably foreseeable injury.

When employees travel and/or are posted internationally, the employer's duty of care becomes more complex, requiring intelligence and risk-management activities beyond the usual requisites that exist in the employee's country of residence. As discussed in Chapter 2, threats to international business travelers and expatriates are multifarious and growing. When these are coupled with extensive legal and statutory regimes requiring a stringent standard of care from employers, the need

to take appropriate steps to ensure the health, safety, and security of their employees is clear. The alternative—as shown in numerous cases—is to face litigation, legal penalties, hefty fines, and even imprisonment for corporate decision makers.

Legislation and case law across Western countries addressing the employer's duty of care has become significantly more developed and complex over the last decade. What follows focuses on laws in the United States, Great Britain, and the European Union (EU), though it is of note that an employer's duty of care is also addressed in legislation and case law in Australia, Belgium, Canada, France, Germany, the Netherlands and Spain. Moreover, this is also a growing feature of emerging markets—even China and India—so the field is moving rapidly.

Relevant Laws in the United States

An employer's duty of care in the United States is addressed through both statutory schemes and common law. Two relevant statutory sources of law address an employer's duty of care to its employees. The first is the Occupational Safety and Health Administration Act of 1970 (OSHA). The second is state *workers' compensation* laws. OSHA's "general duty clause" mandates that, in addition to compliance with hazard-specific standards, all employers have a general duty to provide their employees with "a workplace free from recognized hazards likely to cause death or serious physical harm." OSHA also requires most large businesses to implement an emergency management plan, and corporations are subject to significant liability if they do not meet certain basic obligations. Those requirements range from emergency reporting to rescue plans to alarm notification systems and training. Interestingly, unlike similar legislation in some other Western countries, OSHA does not apply to extraterritorial job assignments—only domestic work assignments. Thus, OSHA does not require US employers to ensure safe workplaces outside the United States. Non-US companies should note, however, that they are subject to OSHA's general duty clause for any employees on post in the United States.

Workers' compensation laws vary from state to state and generally contain a provision stating (in some variation) that workers' compensation is the full and exclusive compensation for any compensable bodily injury, occupational disease, or resulting death arising out of and in the course of the employee's employment. In laymen's terms, the application of a worker's compensation statute means that damages under the scheme are an employee's only remedy for an injury suffered in the

course of employment; (s)he may not sue for further damages. Employers carry workers' compensation insurance to provide employees with wage replacement and medical benefits in the event of an injury suffered in the course of employment. In contrast to OSHA, some workers' compensation statutes apply extraterritorially to traveling employees, and/or employees posted internationally. For example, Washington DC's workers' compensation statute (DC Code Ann. §§ 32-1501) includes coverage for "traveling employees." The effects of this—and a practical example—are shown in the case of *Khan v. Parsons Global Services, Ltd*., discussed in the accompanying sidebar.

KHAN V. PARSONS GLOBAL SERVICES, LTD.

The issue of worker's compensation applying overseas was addressed in the case of *Khan v. Parsons Global Services, Ltd.* In this case, the plaintiff, a British citizen and employee of defendant Parsons (which was based in Washington, DC), signed an employment contract under which he agreed to work as an accountant for the defendant in Manila, the Philippines. The agreement contained a clause requiring Mr. Khan to accept workers' compensation benefits as "full and exclusive compensation for any compensable bodily injury, occupational disease, or death resulting therefrom, arising in an out of [Mr. Khan's] employment hereunder." Shortly after arriving in Manila with his family, Mr. Khan was kidnapped while walking back to his hotel. He was held for approximately three weeks and went through a harrowing ordeal during which he was tortured, and ultimately had his ear cut off by the kidnappers. Video footage of Mr. Khan losing his ear prompted Parsons to pay the demanded ransom, and Mr. Khan was released.

Mr. Khan and his wife sued Parsons under common-law theories of negligence and intentional infliction of emotional distress, arguing that Parsons improperly conducted negotiations with the kidnappers, delayed payment of the ransom, and refused to provide Mrs. Khan with information about the kidnapping. The plaintiffs argued that the workers' compensation statute was not applicable and that they were not limited to workers' compensation benefits because the kidnapping did not arise out of or occur in the course of Mr. Khan's employment. The bases of these arguments were that

his travel for relocation to Manila had occurred several days before, his job did not involve travel, and his kidnapping occurred on a non-working day after a nonbusiness dinner.

Parsons denied the claims, arguing that plaintiffs were limited to workers' compensation recovery pursuant to the employment agreement, precluding any negligence claims or others brought based on common law. The DC Circuit Court agreed with the plaintiffs, finding that the injuries did not "arise out of or in the course of" Mr. Khan's employment. As a result, Mr. Khan was permitted to sue Parsons under negligence and other common-law theories, rather than being limited to remedies under the workers' compensation statute. In so finding, the DC Circuit Court discussed similar laws in Virginia, California, New York, and Minnesota. Although not dispositive, *Khan* demonstrates that *both* workers' compensation statutes and broader common-law causes of action under US law may be used to hold employers liable for injuries sustained by employees while posted internationally.

As the *Khan* case demonstrates, in addition to liability under legislative schemes, employers are also held to a standard of care under US common law, most often through *common-law claims for negligence*. The basic elements of a common-law negligence cause of action are

- A duty under the law
- A breach of that duty
- The failure to exercise the standard of care of a reasonably prudent person/company in similar circumstances
- Damages that are proximately caused by the breach

Common-law negligence causes of action require an employer to exercise reasonable care to protect and mitigate against *reasonably foreseeable* dangers to employees. Whether a danger is reasonably foreseeable depends on the facts of the case at hand. The *Khan* case provides one such example: The court allowed the plaintiffs to go forward with a common-law negligence claim on the theory that Parsons should have taken greater steps to protect the employee from an arguably reasonably foreseeable injury. Similarly, in *Hicks v. Waterman Steamship Corp. & Maersk Line, Ltd*., the plaintiff, a steward on a ship who was allegedly injured during its hijacking by Somali pirates, sued under the Jones Act and general maritime and common

law, alleging that defendants "knowingly sent their employees…into pirate infested waters…knowingly exposed their employees to grave and imminent danger…and did not take adequate steps to provide appropriate levels of security and safety for their employees." (Note that the final merits of *Hicks* have not been adjudicated at the time of writing.)

An additional illustrative case addressing whether injuries are "reasonably foreseeable" is *Enlow et al. v. Union Texas*. In *Enlow*, the survivors of four employees who were murdered in Pakistan sued the defendant oil company, alleging that it breached its duty of care. The plaintiffs claimed that the employer did not have a persuasive need to send the employees to Pakistan during a time of instability and in the face of pervasive anti-US sentiment in the country. The plaintiffs also alleged that the oil company failed to provide the employees with an essential level of security. The jury determined that the oil company employer had not breached its duty of care because the risk that the employees would be murdered while in Pakistan was not foreseeable, and that the employer had also taken reasonable steps to ensure security, including the retention of a private risk management firm.

Khan, *Hicks*, and *Enlow* demonstrate that common-law negligence causes of action are fully available to employees, and that employers that fail to investigate and protect employees against reasonably foreseeable dangers may be held liable under US civil law for such failures. Assessing potential risks requires evaluation of threat and vulnerability; in security terms, these are the responsibilities of intelligence and operations teams, respectively. (Operations teams will also recommend appropriate mitigations dependent on the outcome of the analysis, as we will discuss in greater detail later in the book.) Ergo, this is a mandate for some form of clear threat assessment process involving intelligence. It is notable that in *Enlow*, the jury found for the company in part due to the fact that they had retained ongoing risk management advice. Moreover, the current operational environment mandates some form of regular review, since, as discussed in Chapter 2, threats are now more networked and are evolving faster than ever before. Not keeping up to date with developments could be seen as clear grounds for negligence, based on the current case law, and so it is perhaps no surprise that monitoring of travelers and assets overseas to protect from country-risk factors is one of the main activities of security intelligence analysts in many companies.

Employers may also protect themselves legally and meet their standard of care by providing relevant training and security protection to employees posted in volatile areas of the world. A pertinent example is provided

by the case of *Curtis v. Beatrice Foods Co.* The plaintiff in *Curtis* was the manager of an industrial company incorporated in Bogota, Colombia, the defendant parent company of which was based in Chicago. The plaintiff was kidnapped on the streets of Bogota and held for eight months until the parent company paid a ransom of approximately $500,000 for his release. The plaintiff sued under Colombian law, alleging that the defendant did not "do well enough" on his behalf during the ransom negotiations. Ultimately, the court found that the plaintiff, though well aware of the risk of kidnapping, did not do enough to protect himself. The plaintiff had spent most of his adult life living in Latin America and knew that Bogota was in a state of great unrest. He had been warned by the US embassy in Bogota that he might be a kidnapping target, and his employer provided him with training on how to mitigate against the dangers of kidnapping. Indeed, the court noted that "[defendant] had schooled [plaintiff] on how to protect himself from the threat of kidnapping, and had put an expert agency at his disposal…to help him if need be." Based on these facts, the court held that the employer had not breached its duty to the plaintiff. The *Curtis* case therefore drives home the fact that employers must be aware of all attendant risks of sending their employees to work abroad, again emphasizing the need for an intelligence-led process to ensure that prevention, protection, and preparation activities are as effective as possible.

Relevant Laws in the United Kingdom

Laws addressing an employer's duty of care are much more stringent and highly developed in the UK. Where the United States has only civil remedies for an employer's breach of the duty of care, employees may seek redress in the UK through both civil and criminal avenues. The UK does not have a comparable workers' compensation scheme. Civil actions for injuries suffered by employees in the course of employment in the UK are usually based on the Health and Safety at Work Act of 1974 (HSWA, equivalent to OSHA), and also on common-law causes of action based on a general duty of care. The duty under HSWA is similar to that under OSHA. The relevant section states that "[i]t shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his/her employees." Unlike OSHA, HSWA expressly applies extraterritorially, so employers in the UK can be held liable for injuries sustained by employees outside the UK.

Criminal suits based on an employer's breach of the duty of care are brought under the UK Corporate Manslaughter and Corporate Homicide

Act 2007 (Manslaughter Act). The act, which went into effect in 2008, has attracted much attention throughout Europe and the United States. It therefore has wide importance, as it seems likely to lead the way in a global trend for criminalizing breach of the duty of care to employees. An organization is liable under the Manslaughter Act "if the way in which its activities are managed or organized (a) causes a person's death, and (b) amounts to a gross breach of a relevant duty of care owed by the organization to the deceased." The death need not specifically be that of an employee; the statute applies to deaths of other persons such as people on work sites and travelers. Under the act, a "breach of duty of care by an organization is a 'gross' breach if the conduct alleged…falls far below what can be reasonably expected of the organization in the circumstances." The act applies to a wide range of organizations, including corporations, government departments, partnerships, trade unions, employers' associations, and the Crown. An employer need not be registered in the UK to be subject to the act; it simply requires that the work-related death occur in the UK (or anywhere in the world, for a UK-registered company).

An important component of the Manslaughter Act is found in the fact that it does not require proof that one individual was responsible for the death. In contrast, the HSWA allows for a company to be convicted of manslaughter, but only if a "directing mind" of the organization is individually guilty of the offense. In practice, this has limited the applicability of the clause in the United States, since individual responsibility is hard to define. The Manslaughter Act does, however, require that the breach of the duty of care originate at the senior management level for corporate culpability. The Manslaughter Act also applies extraterritorially—it simply requires that the decision leading to the breach of care occur within the UK, regardless of the location of the incident.

The penalties for culpability under the Manslaughter Act can be severe. Convicted organizations may be ordered to pay fines upon which the act does not impose a monetary limit, and courts may dictate remedial actions and require convicted organizations to publicize their failings and state how they intend to avoid such negligence in the future. The reputational ramifications for a company can therefore be dire. Because the act is relatively new, the full scope of its reach is not yet known. An article dated January 28, 2013, from *The Telegraph* (Gosden 2013) states that forty-five cases were filed under the act in 2011 and sixty-three in 2012, potentially showing increasing awareness of how to apply the law. According to the article, three convictions have been recorded, and fifty-six cases are ongoing.

Common-law causes of action for negligence are also available to employees who bring suit in the UK. Similar to those in the United States, common-law causes of action brought in the UK based on an employer's breach of its duty of care require that the risk that caused the injury or death be "reasonably foreseeable." Again, this effectively mandates that employers have effective risk-identification processes in place that are based on sound intelligence functions.

LONGWORTH V. COPPAS INTERNATIONAL LTD.

Longworth v. Coppas International Ltd. lays out important tenets regarding an employer's duty of care under UK law. In *Longworth*, the plaintiff, a widow, sued the employers of her deceased husband, a former employee of the defendant. In the course of his employment, the plaintiff's husband was based in Basra, Iraq, when hostilities broke out between Iraq and Iran in September 1980. Plaintiff's husband was killed when an Iranian bomb struck the garage facility in which he was working. The plaintiff averred that the defendant employer breached a duty of care to her husband and other employees by failing to protect them from unnecessary risk, because the defendant knew or should have known that the employees were at risk of attack from Iranian missiles. She further alleged that after hostilities broke out, the employer had a duty to evacuate its employees from the area. With regard to the requisite duty of care, the court held that:

> [T]he basic duty of an employer is to take reasonable care that the employee is not exposed to unnecessary risks. Proper compliance with that duty requires the employer to pay attention to the risks to which the employee is, or may be, exposed, and to pay reasonable attention to other relevant circumstances. It has been recognised that the general duty of an employer extends to protection of an employee against natural hazards of which the employer knows or should anticipate.… Accordingly, if an employer learns that his employee's place of work has become part of a war zone and that the employee's safety is imminently threatened by the activities of the combatants, I find nothing…which would excuse the employer from the duty of assessing the risk and in appropriate circumstances of advising, exhorting, or even of enjoining his employee to quit the danger area.

The plaintiff in *Longworth* ultimately did not recover damages because the court found that the missile attack was occasioned by an independent third party, and the employer, in order to be liable, had to have known that the attack was very likely to occur. The court found that the defendant could not have had such knowledge, and the claim was therefore dismissed. *Longworth* does, however, provide important instruction on the need for an employer to be proactive and stay well informed of the circumstances under which and the areas in which its employees are working abroad.

Relevant Laws in the European Union

Regulations and treaties control an employer's duty of care under the laws of the EU. Two in particular are of import, and they address directives related to the safety and welfare of workers, and the directives related to jurisdiction and applicable law. Directive 89/391/EEC (12 June 1989) gives a very broad, general framework for an employer's obligation to prevent occupational risks, promote safety and health, and eliminate risk and accident factors. The second pertinent directive is one related to the posting of employees. The Directive on the Posting of Workers, Directive 96/71/EC, protects workers posted to another EU member state on a temporary basis. The directive requires, at the very least, that posted employees enjoy certain minimum terms and conditions of employment that apply to workers in the member state (working hours, vacation, wages, duty of care), regardless of the law applicable to the employer–employee relationship. It also permits the posted employee to bring suit in the country where the worker is stationed.

Developing Causes of Action: Negligent Failure to Plan

A currently developing area of common-law negligence revolves around the so-called negligent-failure-to-plan cause of action. These cases are sure to become more common, and companies should pay close attention to this area as they build their emergency-response and business-continuity plans. At a basic level, a cause of action for negligent failure to plan expands on the notion that employers have a duty of care to their employees and that the development of crisis-management, emergency-response, and business-continuity plans necessarily falls within that standard of care. A

recent US case illustrates the development of this area of law. In July 2011, a Louisiana judge gave preliminary approval for a $25-million class-action settlement lawsuit against Tenet Healthcare Corporation—the company that owned Memorial Medical Center in New Orleans, Louisiana, when the city was devastated by Hurricane Katrina. The suit alleged that the defendant failed to prepare for and respond sufficiently to a foreseeable disaster: a hurricane in New Orleans. The power went out in the hospital after its backup generators failed, and helicopters did not arrive to aid those inside until two days after the streets flooded. The bodies of forty-five patients were found at Memorial Medical Center after the storm. Doctors admitted to hastening the deaths of some patients by injecting them with drugs. Based on the facts, the judge called the proposed $25-million settlement "fair, reasonable and adequate."

Acts of terrorism, natural disasters, and countless other scenarios require crisis management and emergency response planning, and unfortunately, as these events continue to occur and become more common, courts will be more likely to find that they are "foreseeable," and should therefore be mitigated against in advance. Yet, despite the example in New Orleans, Superstorm Sandy nearly caused the same results at a hospital in New York City. Given the increasing availability of information on these issues, judges and juries are likely to take an increasingly dim view of organizations that do not show a thorough risk awareness and assessment process. In this regard, the intelligence activities around "red-teaming" and scenario planning, discussed in Chapter 13, are of particular importance.

Duty of Care: Summary

The legal frameworks guiding courts on an employer's duty of care obviously vary greatly. At a base level, an employer has an obligation to provide for the health, safety, and security of its employees. Legal schemes range from the very general (in the United States) to the very stringent (in the UK), and the trend is definitely heading toward increasing obligation in this regard. Based on these principles, employers (especially those operating globally) should err on the side of elevating their duty of care standards to the highest possible level to ensure compliance across jurisdictions. In practice, sound risk assessment based on intelligence is required and has proven useful for companies seeking to defend themselves against charges. Conversely, it is increasingly likely that companies

that do not have an effective process for evaluating threats, especially in fast-moving environments, will have fewer defenses when trying to plead their case.

CORPORATE RESPONSIBILITY, COMPLIANCE, AND BUSINESS ETHICS CONCERNS

Corporations, both domestic and multinational, must also be aware of regulatory schemes affecting corporate responsibility, compliance, and business ethics concerns. These include antibribery legislation and awareness of sanctions regimes. This section therefore addresses antibribery laws and sanctions regimes in the United States and UK as well as the intelligence implications of operating within the relevant legislative frameworks.

US Law: The Foreign Corrupt Practices Act

Corruption and bribes in business transactions have been globally pervasive problems for a great many years. In the past decade, however, US enforcement agencies have beefed up anticorruption efforts, most notably using actions based on the Foreign Corrupt Practices Act (FCPA). In general, the FCPA prohibits offering to pay, paying, promising to pay, or authorizing the payment of money or anything of value to a foreign official in order to influence any act or decision of the foreign official in his or her official capacity or to secure any other improper advantage in order to obtain or retain business (the antibribery provisions). The US Department of Justice has published a layman's guide to the FCPA, which acts as a useful resource for individuals and businesses alike.

In order to trigger liability under the FCPA, five elements must be present:

1. An individual acting on behalf of an issuer; "domestic concern"; or those falling within the jurisdictional requirements of the FCPA
2. Corrupt intent
3. A "foreign official"
4. A benefit
5. Satisfaction of the "business purpose test"

With regard to the first prong, the FCPA applies to three categories of individuals: (1) issuers, (2) domestic concerns, and (3) those falling under the territorial jurisdiction of the statute. An *issuer* is, in practice, a company

with a class of securities listed on a national securities exchange in the United States, or a company that is required to file regular reports with the Securities Exchange Commission (SEC). A *domestic concern* is "any individual who is a citizen, national, or resident of the United States; and any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship which has its principal place of business in the United States or which is organized under the laws of a state or territory of the United States." Finally, when territorial jurisdiction is triggered, the FCPA applies to certain foreign nationals or entities not considered issuers or domestic concerns. Territorial jurisdiction applies when a foreign person or entity, either directly or through an agent, engages in any act in furtherance of a corrupt payment while in the territory of the United States. It should be noted that officers, directors, employees, agents, or stockholders acting on behalf of an issuer, domestic concern, or entity triggering territorial jurisdiction may be prosecuted under the FCPA.

The second element of an offense under the FCPA requires "corrupt intent." To violate the FCPA, an offer, promise, or authorization of payment must be made "corruptly," that is, with an intent or desire to wrongfully influence the recipient. The intent must also be willful; the actor must be acting with the knowledge that his conduct is unlawful. It is worth noting that the corrupt act does not need to succeed in its purpose, however. Nor does the recipient (a "foreign official" under US law) need to solicit or accept the payment or bribe. It is enough that the actor formed the willful intent to wrongfully influence.

Under the FCPA, entities are only prohibited from making corrupt payments to "foreign officials" (as opposed to the regulatory scheme under the UK Bribery Act, detailed in the next subsection, which also prohibits corrupt payments to private individuals and businesses). The act defines "foreign official" as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of" any of the above listed entities.

The fourth prong requires a benefit or a promise of a benefit—an "offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to a foreign official." Case law and Department of Justice (DOJ) commentary on the act make clear that an improper benefit can take many forms. Cases most often involve payments of cash, though many others have involved

the provision of exorbitant travel expenses and expensive gifts. There is no minimum threshold amount for corrupt gifts or payments under the FCPA.

The final prong of a cause of action under the FCPA requires satisfaction of the "business purpose test." The FCPA only applies to payments made to "assist an [entity] in obtaining or retaining business for or with, or directing business to, any person." This provision is broadly interpreted by the DOJ and includes payments to obtain or retain government contracts, obtain favorable tax treatment, and a wide range of other actions to secure an unfair business advantage.

Potentially most important for FCPA considerations within an intelligence framework are payments to third parties "while knowing that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly, to any foreign official, to any foreign political party or official thereof, or to any candidate for foreign office" for willfully corrupt purposes. These acts will trigger liability under the FCPA. Due diligence to ascertain the legitimacy and veracity of third-party agents in this context is a vital element of an FCPA compliance program.

There are certain exceptions and affirmative defenses to liability under the FCPA. The FCPA contains a narrow exception for payments for "routine governmental action." These payments, often termed "grease payments," are payments to a foreign official to expedite or secure the performance of routine, *nondiscretionary*, government action. Examples of such action include obtaining permits and licenses to qualify a person or entity to do business in a foreign country; processing governmental papers such as visas and work orders; and providing phone service, power, and water supply. Two affirmative actions to prosecution also exist under the act: (1) the payment is lawful under the written laws of the foreign country; and (2) the payment is made for "reasonable and bona fide expenditure[s]" related to the promotion, demonstration, or explanation of a company's products or services, or are related to a company's performance of a contract with a foreign government.

Penalties under the FCPA can be severe, and both civil and criminal proceedings can be initiated by the DOJ and the SEC. Individuals can face up to five years in prison and fines of up to $100,000. Corporations and businesses can face fines of up to $2 million.

United Kingdom Law: The UK Bribery Act

The UK Bribery Act of 2010 (UKBA) went into effect in 2011 and has had a major effect on both UK businesses and businesses based abroad

that conduct business in the UK. It has been described by the director of the UK's Serious Fraud Office as the "toughest bribery legislation in the world." The jurisdiction of the UKBA reaches organizations incorporated or formed in the UK as well as individuals who are UK nationals or ordinarily residents of the UK who commit an act that violates the UKBA, regardless of whether it happened inside or outside the country. Non-UK organizations can also be held liable under the UKBA if they carry on business or part of a business in the UK, regardless of where in the world the organization is formed or based.

There are four key offenses under the UKBA:

1. Bribery of another person
2. Accepting a bribe
3. Bribery of a public official
4. Failure of commercial organizations to prevent bribery

The offense of bribery of another person criminalizes the act of offering, promising, or giving financial or other advantage to another person with the intent that the other person "perform improperly a relevant function or activity" or to reward the person for such conduct. It is imperative to note that, unlike the FCPA, this section of the UKBA applies to *both* public and private sector transactions. In determining whether a function or act has been performed improperly, the standard is what a reasonable person in the UK would expect in relation to the performance of that function or activity.

Because the UKBA criminalizes bribery in the context of private-sector transactions, it also explicitly criminalizes the passive act of accepting a bribe. An individual can be prosecuted if he or she requests, agrees to, receives, or accepts a financial or other advantage intending that, as a result, a relevant function or activity will be performed improperly.

Like the FCPA, the UKBA prohibits the bribery of a foreign official. An offense is committed under this section where a person "offers, promises, or gives financial or other advantage to a foreign public official with the intention of influencing the official in the performance of his or her official functions." The person offering the bribe must intend to obtain or retain business or an advantage in the conduct of business—a standard similar to the business-purpose test under the FCPA. The UKBA defines foreign public officials as "officials, whether elected or appointed, who hold a legislative, administrative, or judicial position of any kind in a country or territory outside the UK." The definition also includes officials of local or municipal governments and those who exercise a public function for

any public agency or public enterprise (such as individuals working for public health agencies).

Finally, the UKBA contains a strict liability offense for failure of a commercial organization to prevent bribery. The FCPA does not contain such a provision. Generally, a rule specifying strict liability makes an entity legally responsible for its actions regardless of intent and without a finding of fault. Under this section of the UKBA, a commercial organization will be liable for failing to prevent bribery "if a person associated with it bribes another person intending to obtain or retain business or an advantage in the conduct of business for that organization." The commercial organization will have a full defense to this cause of action if it can show that, despite a particular case of bribery, it had adequate procedures in place to prevent persons associated with it from bribing. Only a "relevant commercial organization" can commit an offense under this section, and is so defined as "a body or partnership incorporated in the UK irrespective of where it carries on business, or an incorporated body or partnership which carries on a business or part of a business in the UK irrespective of the place of incorporation or formation." Thus, any corporation conducting business in the UK could fall victim to this law. UK courts invoke a "common sense approach" to determine whether an organization carries on business in the UK, taking into account all relevant facts and circumstances. Under this section, the definition of an "associated person" is far reaching and includes one who "performs services for or on behalf of the organization." This definition obviously reaches employees, agents, and subsidiaries, but can also include contractors, suppliers, and those entities included at every level of a supply chain.

In a difference between UK and US law, facilitation payments are prohibited under the UKBA. As stated previously, an affirmative defense to prosecution under the UKBA exists for organizations that have adequate procedures in place to prevent bribery.

Finally, penalties under the UKBA are much more severe than those under the FCPA. Individuals or organizations convicted of the offenses of bribing another or bribing a foreign official can face unlimited fines, and individuals can receive jail sentences of up to ten years. An organization convicted of failure to prevent bribery can face unlimited fines.

Bribery risks and punishment for violations of antibribery laws can be mitigated and avoided through proper due-diligence procedures, which are also mandated by various regulatory compliance regimes too numerous to mention here. The dangers associated with due-diligence failures in this arena are best illustrated through FCPA enforcement

INTELLIGENCE IMPLICATIONS OF ANTIBRIBERY LAWS IN THE UNITED STATES AND UK

Effective compliance with antibribery laws entails many factors, most importantly risk analysis and due-diligence functions. With regard to risk analysis, organizations must be cognizant of where they are exposed to significant risks and how best to mitigate those risks. The most commonly encountered risks for bribery arise in the following categories:

- *Country risk*: This comes into play when operating in countries with high levels of corruption and/or countries without effective antibribery legislation.
- *Sector risk*: Many corporate sectors present higher levels of bribery risk than others (e.g., mining and large-scale infrastructure).
- *Transaction risk*: Some transactions present higher levels of risk (e.g., those that involve charitable giving).
- *Business partnership risk*: Certain relationships may present higher risks, such as those that require intermediaries when dealing with foreign public officials, or where associated third parties are linked to prominent public officials.
- *Human resources risk*: Especially within the context of strict liability under the UKBA for failure of a commercial organization to prevent bribery, it is imperative that an organization be aware of its employees' backgrounds and responsibilities in the context of whether corrupt activity is likely.

Source: The Bribery Act 2010–Guidance.

actions involving *successor liability*. As a general proposition under US law, when a company merges with or acquires another company, the successor entity assumes the predecessor's liabilities. Liabilities under the FCPA are no exception. The DOJ and SEC encourage companies to conduct thorough pre-acquisition due diligence to improve FCPA compliance and to responsibly address any potential liability under the FCPA. A failure to do so can have dire consequences for the acquiring company, as laid out by the DOJ in its *Resource Guide to the U.S. Foreign Corrupt Practices Act*. Contracts obtained by the target company through bribes may be legally unenforceable; business obtained illegally through bribes may be lost; there may be liability for allegedly illegal prior conduct; and the prior acts

may harm the acquiring company's reputation and future business prospects. Additionally, the consequences of FCPA violations uncovered during the due-diligence process can be handled by the acquiring company and the DOJ/SEC through negotiation and remediation—often resulting in no action against the acquiring company for the violations.

Sanctions Regimes in the United States and United Kingdom

Sanctions laws in the United States apply independently of other regulatory schemes such as those discussed previously—including the FCPA and anti-money-laundering laws. The US government imposes economic sanctions against several countries and a large number of individuals and various entities. The sanctions regime in the United States is administered by the Department of Treasury's Office of Foreign Assets Control (OFAC). The OFAC website contains summaries of the controlling laws as well as information regarding how those laws apply in practice (see www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx). OFAC imposes comprehensive sanctions again Cuba, Iran, and Sudan, and also has more targeted sanctions programs against other countries, including North Korea and Syria. OFAC also imposes restrictions against nongovernmental entities and some individuals, termed *specially designated nationals* (SDNs). The list of SDNs includes designated terrorists and terrorist groups, weapons and narcotics traffickers, and a large number of vessels. A comprehensive, frequently updated list of SDNs is published at www.ustreas.gov/offices/enforcement/ofac/sdn/index.shtml.

Generally, US sanctions laws must be complied with by "US individuals," a definition that includes US citizens or permanent residents (wherever located), US companies and foreign branch offices of US companies, and foreign persons located in the US (e.g., non-US citizens working for US companies). US sanctions laws generally prohibit or restrict the provision of goods or services to targeted countries, individuals, or entities. Penalties for violation can be severe: civil penalties of up to $250,000 or twice the amount of the transaction (whichever is greater) as well as criminal penalties for willful violations of up to $1 million per violation and/or imprisonment. Nonmonetary consequences include reputational damages (OFAC penalties are made public) and harm to companies' relationship with the US government.

The United Kingdom follows the sanction schemes put into place by the United Nations and the European Union. When a sanction is set by the UN and/or the EU, the British government takes steps to implement that

sanction in British law. In the UK, the Foreign & Commonwealth Office (FCO) administers the UK's policy on sanctions and embargoes. Like the United States, the UK, EU, and UN publish comprehensive lists of sanctions in force. For example, a consolidated list of financial sanctions targets in the UK can be found at http://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.htm. The UK sanction regime requires absolute compliance, and there are substantial civil and criminal penalties for failure to comply. The maximum penalty is seven years in prison, an unlimited fine, or both. However, like in the United States, the wider reputational damage for companies is potentially the most devastating angle, and this can be very difficult to repair.

Corruption, Compliance, and Sanctions—Summary

Consideration of the various issues at work emphasizes the need for screening along with effective depth and investigative due diligence, which we will discuss again in Chapter 13. For now, it is important to note that the various corruption acts, coupled with the need for regulatory compliance that goes above and beyond the minimum due to duty of care to the organization, are major drivers for the increasing focus of intelligence teams on this topic in a wide range of industries, also evidenced by the ever-increasing base of suppliers of outsourced services.

CONCLUSION: THE LEGAL IMPERATIVE

There are a number of reasons why the legal and regulatory environments are increasingly driving an uptake in the use of corporate security intelligence:

- Laws are becoming ever more stringent, led mainly by the UK, but with this trend being echoed worldwide, including in developing countries.
- Public expectations—and, by extension, those of juries—are increasingly demanding in regards to corporate responsibility and ethics.
- Much rides on whether risks are "reasonably foreseeable"; given the increasing access to information, this definition is now very wide-ranging, and trends again show that expectations are increasing.

- We are increasingly hearing that "compliance is not enough"; companies must now go beyond the bare minimum in order to satisfy would-be investigators that they have taken their responsibilities seriously.
- As more and more organizations adopt intelligence-led approaches, it is becoming harder for those that do not to justify any lack of situational awareness.
- Understanding threat is a critical component of analyzing risks; although the latter is what is mandated, it is impossible to do this without intelligence, despite this often being overlooked (for example in the ISO 31000 standard, discussed in Chapter 4).

We will look at how this works in practice in Chapter 13, which discusses various case studies related to the top-level issues driven by legal and regulatory issues, including duty of care.

4

Operational Drivers for Corporate Security Intelligence

CHAPTER OBJECTIVES

1. To outline the financial and practical benefits of an intelligence-led approach to security.
2. To describe how intelligence helps an organization prevent incidents.
3. To show how intelligence helps drive appropriate protective measures.
4. To demonstrate the role for intelligence in helping prepare the organization.
5. To suggest ways in which intelligence can help drive profits, becoming a key business enabler rather than a cost center.

INTRODUCTION

Chapter 1 outlined the top-level practical benefits of having a corporate security intelligence function. As a reminder, these were as follows:

- To better focus finite security resources
- To inform the alert level status

- To enable security to be proactive rather than reactive
- To provide an estimate of threat response effectiveness
- To identify potential targets for in-depth investigation
- To validate an existing risk-management program
- To expose gaps in your protection (vulnerabilities)
- To determine how effective a particular action has been in degrading an adversary's capability

Ultimately, though, the cold-blooded equation for an organization adopting something that is not forced upon it by the sorts of measures discussed in the previous chapter boils down to one main reason: return on investment. This factor applies to security as much as any other business function. In fact, since security is viewed as a cost center or as overhead in most businesses—essentially being tolerated as a regrettable necessity—it is under particular pressure and scrutiny. So when the chief security officer (CSO) requests money to develop an intelligence function, as with any other expenditure, the expectation is that the CSO will demonstrate a sound financial and practical argument. Obviously, the implications of failing to meet legislative requirements are clear, but as described previously, these requirements are rarely, in themselves, absolute.

The financial arguments regarding security intelligence boil down into two main categories: either to save money or to make it. Naturally, a variety of considerations apply under each heading, so we will therefore consider each of these in more detail later in this chapter.

There is one final consideration: ethics. Arguably, much behavior that is really linked to ethics is now covered by legislation (Duty of Care or the FCPA being great examples), as discussed in Chapter 3. However, there are a number of ethical considerations that come under what an organization "should" do. As with any corporate argument, you can say that this ultimately relates to making money—restricting staff churn, keeping families happy, and managing other welfare issues are all, of course, of benefit to the bottom line. And yet some ethical considerations transcend money in that tackling them is a cost with no clear financial benefit, but it just would not be considered justifiable for a modern organization to proceed without considering them due to their own code of behavior. These vary dramatically by organization and jurisdiction (with the UK and EU being more likely to see this than the US, where CEOs often still argue that fiduciary duty to shareholders trumps all), so the topic is therefore worthy of extra consideration in the "should do" category.

In this chapter we will therefore examine the following:

- The general operating framework for corporate security intelligence, including examining the relationship between threat and risk
- Ways in which intelligence saves money or allows an organization to do more with the same resources (acting as a "force multiplier")
- Ways in which intelligence can help the business make money—an often overlooked angle, but key to consider when building a business case

GENERAL CORPORATE SECURITY INTELLIGENCE OPERATING FRAMEWORK

In 2003, the UK Home Office developed a new National Counter-Terror Strategy, CONTEST. This consisted of four work strands: *Pursue* terrorists in their operating areas; *Prevent* terrorist attacks; *Protect* the homeland; and *Prepare* for the consequences of anything happening. This was released to the public in 2006 and garnered immediate attention. The Four Ps constitute a simple and effective approach that has been very successful and is remarkably easily to conceptualize and communicate. Its simplicity and elegance may be because Sir David Omand (2010), in his role as the first-ever permanent secretary and security and intelligence coordinator in the UK Cabinet Office, thought up the idea in that home of all good ideas, the bath (although reports are unclear as to whether he also shouted "Eureka!").

Since being released for public consumption, the Four Ps have increasingly entered the corporate security lexicon as a framework for understanding the activities related to organizational resilience, albeit in a modified form. Taking this in mind, the general framework for the security intelligence function is therefore to support resilience activities in three main areas (in priority order):

- *Prevent* threat actors from harming the organization.
- *Protect* the organization from the likely actions of threat actors.
- *Prepare* for the effects on the organization of the likely actions of threat actors.

Pursue is a rather more difficult function to carry out in the corporate environment, and although there are occasions where this has been done (often through legal action), it is simpler to exclude this.

Another general aspect to bear in mind is the *risk equation*. This is quantified in various ways, but one common definition is as follows:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} (\times \text{Cost, if measuring impact})$$

When quantifying risk, these are all numerated. Vulnerability may therefore be expressed as percentage likelihood, as may the threat level. Putting a complex art very simply, organizations rate risk—of all types—based essentially on these sorts of assessments, although this version of the equation is orientated toward security risks.

Taking this a stage further, one can further break down the *threat* component of the equation. This is as follows:

$$\text{Threat} = \text{Capability} \times \text{Intent}$$

Therefore, threat intelligence is principally involved with assessing adversaries' capability, intentions, and perception of the organization's vulnerabilities. This does not apply across the full spectrum of corporate intelligence activity, but is worth bearing in mind when considering most aspects—especially activism, espionage, serious organized crime, and terrorism. Note that vulnerabilities can often be addressed very easily, and in a cost-effective manner, through what we call *synergistic controls*—discussed at greater length later in this chapter.

Finally, a common security assessment framework to be aware of is the *threat*, *vulnerability*, and *risk assessment* (TVRA). This usually takes a specific asset, feature, or event as its focus (let's say an asset here, for the sake of an example). The possible security threats are assessed, and then the vulnerability of the asset is mapped to these threats, being rated on likelihood and impact to determine the risk (as mentioned previously). Typical quantifications are shown in Figure 4.1.

The outcomes give priorities to decision makers in terms of risk mitigation and cost effectiveness. The role of intelligence in this is clear—threat assessment. This most commonly comes into play when considering specific asset protection, but is closely related to red-teaming and executive protection (see Chapter 13). Perhaps most important to note, and a common failing, is that the threat proportion of a TVRA is not static (countermeasures too may change). This emphasizes the increasing need for the intelligence cycle to be networked and adaptive when required. Although periodic assessments may be useful in identifying trends, the system must also be geared for "action-on" intelligence. In the case of a TVRA for a specific asset, a spike in a particular threat

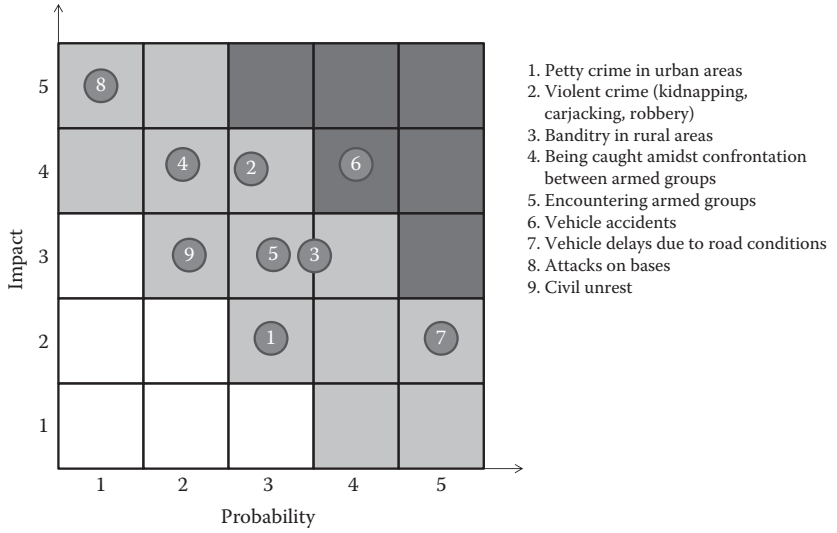

Figure 4.1 Example risk matrix in the form of a Boston square.

may produce an *urgent operational requirement* for mitigation. This is best enabled if the intelligence team and the decision makers work closely and in parallel—a key theme to getting the best results.

RISK-MANAGEMENT STANDARDS

Although a number of international risk-management standards exist, these are mostly related to different business activities. For our purposes, therefore, we will focus on *ISO 31000*. This international standard was published in 2009, and it describes in detail a process for incorporating risk management. There is, however, one major catch: The discussion of risk quantification is very crude (basically saying "use any approved method"). Examination of other literature shows the same trend. For example, the Accenture report discussed in Chapter 2 discussed the importance of understanding geopolitical risks, but similarly glossed over the detail of how to go about this. Business-continuity standards show a similar lack of interest in actually discussing the operational mechanisms of identifying threats in favor of strategic-level processes to deal with issues once discovered.

This therefore highlights a common failing, driven in part by the comparative lack of understanding of how security intelligence actually works and what it can offer. However, this is a critical oversight. The point of having a strategic risk-management framework is surely lost if it is built upon shaky foundations. As shown previously, the "nitty gritty" of identifying and quantifying threats, especially in a predictive fashion, is a key driver of the whole risk equation, which is why it is so good that you're reading this book!

HOW CORPORATE SECURITY INTELLIGENCE SAVES MONEY

The most basic, core component of security is to prevent loss. For a company, the underlying rationale—be it of assets, reputation, people, or money—is always a financial one. The aim is that by investing, say, a million dollars in security capabilities, a larger amount of loss—or assessed potential loss—can be offset. This equation is, incidentally, very much evident in how banks deal with customer losses due to card fraud, and so on: The cost of developing truly and completely effective security would outweigh the costs of just refunding the customers. The balance is always finding a "sweet spot" whereby the spending on security is justified.

This means that any security organization always has more to do than it is equipped, budgeted, or resourced for. An organization would be wasteful (and hopelessly misguided) if it budgeted to be 100% secure. As the threat overview in Chapter 2 showed, this is perhaps the case now more than ever, given the range of challenges brought about by the global marketplace. Therefore, one of the main benefits of an intelligence-led approach is that it offers the opportunity to significantly improve the cost efficiency of not just the security department, but the organization as a whole.

Intelligence applies at the tactical, operational, and strategic levels, and the underlying nature of the activities undertaken does not change, regardless of the audience or purpose. Indeed, as we have said before, many of these activities are already being undertaken by a variety of people within the organization as part of their jobs. The difference is that an embedded process offers the opportunity to bring all of these disparate aspects together to form a real knowledge base—properly assessed and evaluated—in order to improve the organization's ability to respond in a clear and coherent fashion across all of its activities.

It does this in three main areas:

- Enabling a clear and common understanding of the threat/operating environment
- Providing early warning of potential issues
- Offering an "adversary viewpoint" of the organization

An overview of the benefits offered is presented in Table 4.1.

Table 4.1 Benefits of Corporate Security Intelligence

Activity	How	Benefits
Enabling a clear and common understanding of the threat/operating environment	Synthesizing existing information and knowledge from across the business Bringing in external viewpoints and advice Assessing this for probability Sharing this knowledge with decision makers in a timely fashion	Scenario planning—being able to understand various courses of events and implications of actions, ensuring that the business not only remains safe, but can also profit Crisis support Evaluating risk exposure Ensuring that wider trends are incorporated into security and resilience planning Support to strategic decision making
Providing early warning of potential issues	Understanding likely threats and looking for triggers, indicators and warnings Evaluating where business activities may provoke a response Undertaking regular monitoring Examining potential reputational issues	Preventing a potential incident or issues Mitigating the immediate and long-term impacts of an incident or issue Business intelligence/depth due diligence activities to flag potential issues
Offering an "adversary viewpoint" of the organization	Red-teaming Threat, risk, and vulnerability assessments	Ensuring that resources allocated are as effective as possible Aiding in exercising and preparedness Understanding the "most likely" scenario

Added to these considerations, centralizing and coordinating the process of knowledge management often allows substantial efficiencies in expenditure. For example, subscriptions to information services can often be rationalized across the organization, and the information can be offered through a single platform, with appropriate controls and commentary. This almost always offers a quick win for larger organizations. Focusing assessments in one area also offers advantages, since it allows a common response across the organization to emerging threats or issues, although of course this also emphasizes the need for such assessments to be well grounded—another critical reason why intelligence should be implemented properly across an organization rather than as an ad hoc, uncontrolled function, as is so often the case.

HOW CORPORATE SECURITY INTELLIGENCE MAKES MONEY

This is one of the most overlooked benefits to having a corporate security intelligence function, largely because the nature of the security department immediately tends to put it at one remove from doing business. This harks back to the traditional model of security discussed in Chapter 1. As mentioned previously, however, the "new model" sees the function embedded more alongside other business units, with a focus being on the bottom line, and so driving rather than impeding business is the order of the day. In most cases intelligence, more than any other part of the security function, is what offers this capability. The reason for this is that intelligence is in essence about knowledge, and knowledge can translate into power—or, for a business, money.

Some businesses, particularly in the financial sector, are pretty much all about making money through understanding risk better than their competitors. Therefore, it is perhaps no surprise that these companies were some of the first to embrace a security intelligence function, and these companies still have an advantage in this area when comparing across different industries. For banks and insurance companies, geopolitical risk is tied directly to how they profit. The ability to predict the impact of events on countries not only helps safeguard assets, personnel, and investments, but also helps the trading desks or underwriters make accurate assessments. Banks in particular use geopolitical assessments—focused mainly on country-risk factors such as political stability and risk of unrest—to justify the offsets/set-asides of money that

they have to make to underwrite their investments. An example of how the security intelligence function helped one such bank is broken out in Figure 4.1.

Although this is clearest in the financial sector, this advantage applies across most industries. For example, emerging markets are increasingly key at this point in world history, underpinned as it is by increasing globalization and the rapid expansion in the needs and demands of burgeoning populations. Understanding when and how to invest in/develop these markets, ideally before competitors, can offer real operational benefits. Understanding up-and-coming figures of importance can also help to enable business, especially for the longer term. This is why many of the world's largest companies have for years employed ex-diplomats and former intelligence officers in key roles as enablers and advisors, often running networks of correspondents and maintaining their former overseas contacts.

These relationships are not run as part of a security intelligence process, per se, but the function can readily be replicated even in firms that cannot, or will not, establish political advisory posts of this nature. This capability tends to relate to an in-house depth due-diligence/business-intelligence function, more commonly established to understand potential counterparty risk (especially in terms of reputation). The major activity is *power mapping*, long favored by activists and other groups seeking to influence policy. Definitions abound, but the Bonner Foundation's is one of the best:

> Power mapping is a framework for addressing issues and problem solving through leveraging relationships and networks. It is a conceptual strategy of determining whom you need to influence, exactly who can influence your target, and whom you can actually influence to start the dominoes in motion. This framework is based on the assumption that networks of relationships (between individuals, organizations, institutions, etc.) are critical resources, and that stronger networks yield stronger solutions.

We will come back to this in more detail in Chapter 13. Note that a common error is to confuse this with *influence or stakeholder mapping*, which is a distinct concept. This involves analyzing how much someone can influence a given issue and then comparing that to where they stand. In contrast, power mapping involves the study and understanding of networks as well as personalities to get results and reach these key influencers, so the two often work hand in hand.

As an example of the concept in use, imagine a company that has sales personnel regularly traveling to the Arabian Gulf in order to meet

and develop potential leads. In the course of business development, they meet a minor member of a local royal family who claims to have influence. This sounds promising. But is he really as influential as he claims? Time, effort, and substantial amounts of money are often wasted before it turns out that, despite the individual's royal title, this person does not actually offer a real opportunity. Contrast this with an intelligence-led approach whereby the key individuals and potential targets were identified in advance. It might not be possible to get a meeting directly with these people, but crossing their known networks with a list of existing clients might show that there are connections who could usefully facilitate an introduction. Moreover, time, effort, and resources are not wasted pursuing worthless leads. This is predominantly an activity that should be driven by the sales team, but they probably do not have access to the insight, research, knowledge, and sources that a well-set-up security intelligence apparatus could bring to bear. When combined, i.e., when the sales team asks the security intelligence analyst, "We'd like to meet this person; tell us how important they really are and how to get to them," you can see how powerful and economical this approach can be.

We'll go on to discuss the actual mechanism of how to conduct power mapping more in Chapter 5, which examines use cases for security intelligence. For now, though, this is a great example of where the security function can actually serve as a business enabler rather than just being the people who say "no" all the time. This also applies particularly with travel—ensuring that people are safe to the extent that either overhead becomes crippling or all travel is banned is not a great approach. Instead, for example, understanding that the November 26, 2011, terrorist raids on Mumbai did not necessitate shutting down all travel to India for months on end makes a big difference to the bottom line. Walking this line is a hard role for the chief security officer (CSO), but there's no doubt that a security department that is engaged and aware of the bottom-line imperative to business will thrive compared to those that apply a more static, bureaucratic approach. Being led by intelligence is a key part to bringing about that adaptive, enabling approach—not least because when done well, it allows clear and common understanding of even the most difficult situations.

CONCLUSION: INTELLIGENCE AND THE FOUR PS

Overall, a security function of a business is often regarded as something of an insurance policy. To some extent, you have to have it, but you begrudge

paying much for it—until you need it. At that point, you may belatedly regret taking the cheap option (as many people have). A formal security intelligence function is to some extent similarly a more expensive "bolt on" to a basic function. Arguably, in most operating jurisdictions, legislative requirements could be met without it. (Although, as repeatedly argued, any business already has some sort of intelligence function going on; it just doesn't recognize it.) However, the ethical and legislative trend is clearly against an approach of doing "just enough" as regards risk management. Combined with this, the security operating environment for businesses is becoming ever more complex. It is therefore no surprise that more and more large firms are looking to refine their intelligence capability.

There is also an underlying tension in business between being *lean* and being *resilient*. The financial imperative of the present day is for overhead to be as low as possible, especially in businesses where operating units are more or less autonomous. The large central office is therefore increasingly being pared down. This is also evident in the nongovernmental organization (NGO) sector, and even in government. However, this potentially makes organizations significantly more vulnerable to any security incidents that occur, since they may lack the depth to be able to absorb and recover from the blow. Just-in-time production methods, complex interdependencies between companies, and tighter inventory controls also mean that the consequences of unforeseen incidents are greater than ever. Taken together, security functions therefore have to do much, much more with potentially way, way less. This drive toward efficiency clearly points toward overcoming wasteful attitudes and instead shifting toward a leaner, more agile function that is led by intelligence.

Finally, as regards the mission for corporate intelligence work, we can steal a leaf from Sir David Omand and the UK Cabinet Office, going one better with the four Ps:

- Help detect and *prevent* threats.
- Help the organization *protect* itself against credible threats.
- Help the organization *prepare* for likely incidents or even low-likelihood/high-impact situations.
- Help the organization *profit*.

Throughout, intelligence acts as a way to help do more with the resources available. Helping organizations understand threats really helps drive finer understanding of risks, which in turn drives profitability. Intelligence advice is thus enabling as much as it is restrictive, in line with the "new model" of corporate security discussed in Chapter 1.

Section II

Theory

5

The Fundamentals of Intelligence

CHAPTER OBJECTIVES

1. To present the fundamental theoretical ideas underlying all intelligence work, whether in the public or private sector.
2. To demonstrate the knowledge-data hierarchy and explain how data, information, and intelligence are different concepts.
3. To introduce readers to the intelligence cycle and explain why some are critical of it.
4. To introduce the key roles and responsibilities within the intelligence team.

INTRODUCTION

We discussed the aim and purpose of intelligence throughout the Section 1 of this book. To condense and summarize this previous discussion, the aim is to provide accurate, timely, relevant, and, ideally, actionable knowledge and insight into changes in the security environment. Fundamentally, intelligence is a process for dealing with uncertainty, reducing it to as low a level as is reasonably possible given inevitable constraints. This is achieved by collecting relevant information, placing it in context to

provide knowledge, and conveying it in the form of intelligence products to enhance understanding and offer managers a decision advantage. This includes helping the organization *prevent* incidents, *protect* against threats, *prepare* adequately for anything that may occur, and *profit*, whether financially or through being able to successfully undertake its mission.

The fundamentals of intelligence do not vary substantially between national security purposes or corporate security. There are, however, differences in application. While much of what follows will therefore be familiar to anyone with a national security and intelligence background, this chapter will also begin to lay the foundations for a dedicated corporate security intelligence framework, suitable for any organization of any size—something that we will discuss in detail in Section 3 of this book.

A key thing to remember when relating intelligence to the corporate world is that it is particularly important to "talk the language of business." As a result, some of the concepts seen here may well be presented differently in the literature relating to national security intelligence, although the underlying theory is exactly the same. In sum, this is all based on a number of fundamental points:

- Intelligence is not information.
- Intelligence is generated via a disciplined, structured process.
- Intelligence is directly related to the client's needs.
- Intelligence is being comfortable with uncertainty.

There are many more factors to consider, but these are the main things to bear in mind. We will start therefore by looking at the relationship between intelligence and information before going on to talk through process, principles, types of intelligence, and the people required to make this all work effectively.

THE INFORMATION HIERARCHY

One of the most important points for any intelligence practitioner to understand is that there is a very real difference between *information* and *intelligence*. This is even more important to note in today's world, where information—thanks to many successive revolutions in technology—is now available in an unprecedented fashion and can be analyzed in ways that would once have been unimaginable.

Information science is a discipline that has sprung up in response to this burgeoning access to data. In common with much of the theory

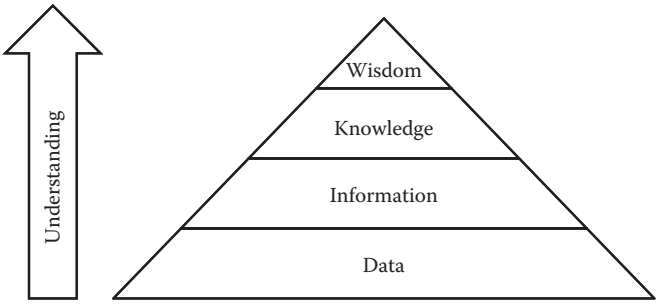

Figure 5.1 The DIKW triangle.

discussed in this section, this topic really began to receive academic attention after the Second World War. The key underlying theory of relevance to us is what is known variously as the *DIKW Pyramid* (Figure 5.1) or the *Information Hierarchy*, to use just two of the many names for the same essential idea. The term *DIKW* refers to the following:

- *Data*: The raw elements of discrete, objective facts or observations, which are unorganized and unprocessed and therefore have no meaning or value because of lack of context and interpretation.
- *Information*: Organized or structured data that has been processed in such a way that the information now has relevance for a specific purpose or context, and is therefore meaningful, valuable, useful, and relevant.
- *Knowledge*: Although this is an elusive concept, definitions include that this is a synthesis of multiple sources of information over time, organized and processed to convey understanding, experience, and accumulated learning.
- *Wisdom*: The highest level of understanding, this is knowledge crossed with judgment.

This is actually a process that we all experience and undertake, although often without realizing it. A practical example of this may therefore help illustrate the concept. Imagine that you are working for an oil and gas firm operating in a high-intensity security environment, such as Iraq or the Niger Delta. The sound of a gunshot is raw data. Your ears, which are conveniently placed to sense distance and range, tell you that it came from *over there*. This is information: a shot was fired, from that location. You realize that you also heard the *crack* of the bullet go past you before you heard the *thump* of the shot. Synthesizing these two pieces of

information gives knowledge—the shot was fired at you! Wisdom, in this case, consists of realizing that another shot is likely to follow; that the shooter might have adjusted their aim; and that a packed earth embankment offers better cover from bullets than a nearby bush. We will look at more intelligence-related angles later in the book, but for now this should suffice to convey the principle.

Various DIKW models exist, and the concept has stirred a large amount of debate, with very little consensus over definitions. The ones portrayed here are generally from Jennifer Rowley's (2007) study of existing material, published as "The wisdom hierarchy: Representations of the DIKW hierarchy," since this represents the widest view. For our purposes, though, the debate is less important than the clear understanding that a process is required to impart wisdom to decision makers (the ultimate goal of intelligence practitioners). This must allow the collection and observation of data (in the form of either facts or signals); the collation of data into meaningful information; the synthesis of information into knowledge; and the conveyance of that knowledge, mixed with judgment, to generate wisdom.

THE INTELLIGENCE CYCLE

Understanding of the Information Hierarchy shows how intelligence is the end product of a disciplined process whereby raw data is organized, reviewed, vetted, and validated. Historically, this process was not formulated. For example, the Duke of Wellington, when operating in the Iberian Peninsula during the Napoleonic wars, had a highly developed intelligence apparatus that worked to some degree informally. This did not stop it from being highly effective (and often giving him *decision advantage*—well before anyone coined the term). This reflects much of human endeavor at the time, where it was possible to learn on the job, and approaches were inherited and developed based on the competence of the personalities involved. Of course this was also possible only because the level of information actually available at the time was so very low—even maps of the countryside were in scarce supply.

As information became more and more available, usually through the march of technology (especially as regards communications), it drove up the need to have a more structured approach. By the First World War, the terms *collection*, *collation*, and *dissemination* had entered general use in the

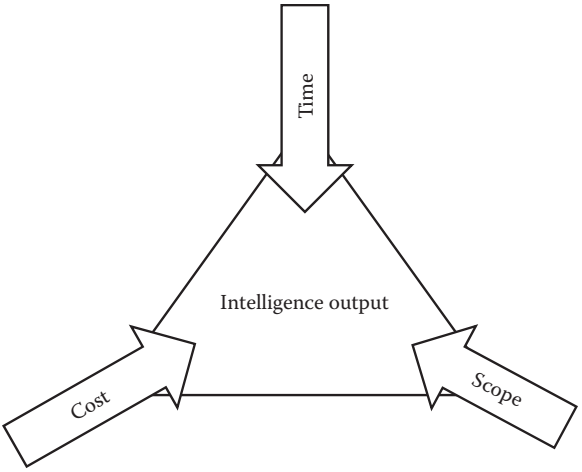

Figure 5.2 The Iron Triangle—how time, cost, and scope constrain the output.

British and American militaries, although there is no evidence that there was an underlying cycle (Jensen, McElreath, and Graves 2012). This seems to be because the huge militaries of the time were able to throw sufficient manpower at the task that they could still get away with an essentially competence-driven, ad hoc approach. It was thus the interwar period that drove a real step toward efficient processes, as information availability and speed of communications continued to increase, and resource availability became ever scarcer. This underlines the basic purpose of a process like this, which is to get the best results possible within the constraints of time and resources, as seen in Figure 5.2.

As with so much other intelligence theory, however, it was the experience of the Second World War that led to the formal development of what is called the *intelligence cycle* (Figure 5.3). Jensen, McElreath, and Graves (2012) discuss how this term first appeared in the book *Intelligence Is for Commanders*, by Roger Glass and Philip Davidson (1948), and speculate that the timing potentially points toward development by the Central Intelligence Agency (almost certainly building on the lessons learned from the Office of Strategic Services during the war). In this regard, the process is firmly founded on what we might now call *best practice*.

The intelligence cycle is represented in various forms today, and is subject to intense debate, although every intelligence function in existence

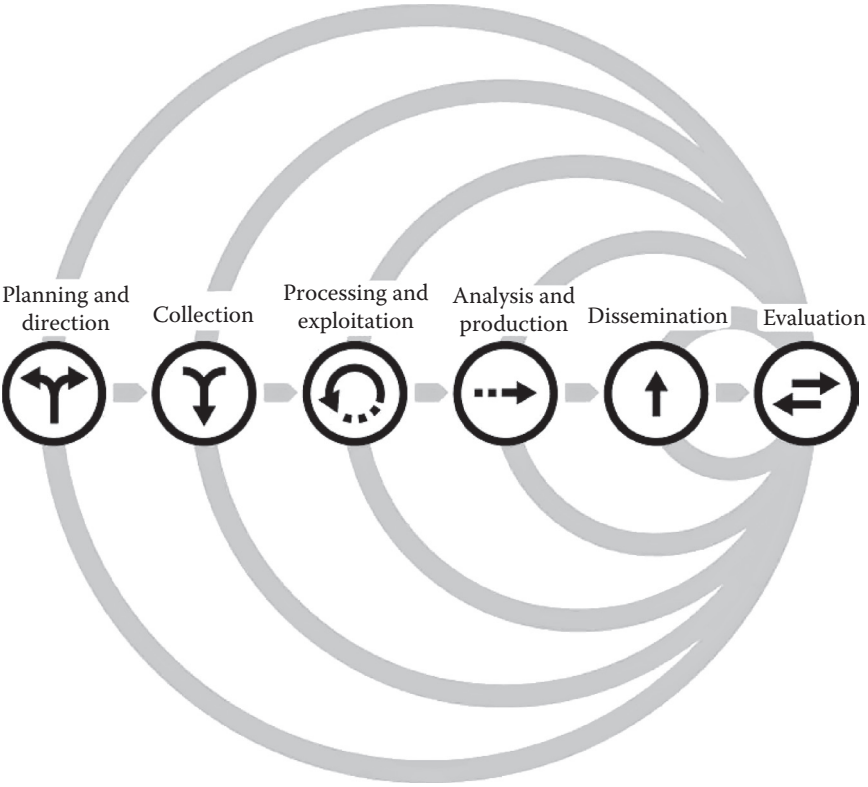

Figure 5.3 Intelligence cycle (ODNI).

almost certainly reflects its underlying logic (Figure 5.3). Traditionally, the cycle has been presented as a wheel of different steps, usually between four and six. Such adaptation reflects how this is a model or framework for understanding, rather than something that is always slavishly adhered to. Often, especially in more informal intelligence setups, the process will be being carried out, but the people involved may have no awareness of the fact at all. This reflects how, to some extent, common sense is at work, and of course some individuals have more innate flair for the work, probably adopting the approach unconsciously. The intelligence community similarly seeks to embed this knowledge into operators rather than to drive everything based on what is essentially a fairly basic framework—and one that is flawed, like any model. However, all such arguments aside, it undoubtedly works.

The most common terms used for the steps/phases of the intelligence cycle, in their usual order, are as follows:

- *Direction*: The first step, sometimes also called the planning phase. This refers mainly to the definition of the questions to be answered by intelligence or the problems being tackled. In the direction phase, intelligence requirements (IRs) are often broken out from the more general priorities of the decision maker or are derived from broader issues that the intelligence team believes should be of interest. The overall task is also defined, and initial plans are made to drive further activities, often including the allocation of resources, derivation of timelines, and identification of critical aspects of intelligence that would necessitate immediate reporting. This step is usually under the aegis of the intelligence manager.
- *Collection*: Once the IRs have been defined, relevant data/information is gathered from a range of sources. Ideally, these should be mutually reinforcing and comprehensive, and *source management* is an ongoing activity for any intelligence team. Material is collected in accordance with the *collection plan*, which outlines who will collect what, by when, and in what format.
- *Collation*: Collation is often overlooked, but it is a highly important stage in producing meaningful intelligence. It is sometimes more broadly referred to as *processing* and *exploitation*, although the former term can cause confusion, as older military doctrine still uses this term also to cover analysis. This stage principally involves keeping information organized and coherent, enabling ready *access*, a term raised by Sir David Omand (2010) in his book *Securing the State*, which is briefly discussed later in this chapter. This includes normalizing and harmonizing data, storing it in a manner in which it can easily be searched and recovered (e.g., a relational database), and providing visualizations.
- *Analysis*: This covers the actual production of refined intelligence material (although in practice, some material may have immediate utility in the collection/collation phases, as discussed later in this chapter). Analysts integrate or *synthesize* data and place it in context, using a variety of tools and approaches to generate understanding and minimize uncertainty for the ultimate client. Their role is, however, to inform the decision maker—not to make the decision.
- *Dissemination*: Once knowledge is gained, it must be communicated to consumers of the knowledge in the form of product.

This entails consideration of channels, methods, operational security/secrecy, presentation formats, and the balance between "pushing" product to clients and them being able to "pull" what they need. Ultimately, the effectiveness of the intelligence function is based on its ability to influence and help guide the decision maker, so this step is critical. All too often, high quality, insightful analysis has failed to reach those who needed it most, or was lost in the more general "noise."

- *Evaluation*: This final feedback step takes us back to where we began—at the direction phase as new intelligence requirements emerge, based on consumers' reading and assessment of what the intelligence function has presented. The model belonging to the US director of national intelligence (DNI), pictured in Figure 5.3, views this as a constant part of the process, and this view is gaining more and more traction.

Criticism of the Intelligence Cycle

Ultimately, any model is an attempt to reduce complexity to a usable form. Many of the discussions over the intelligence cycle are thus inherently purely theoretical and have little practical impact. That said, while it undeniably has utility, the intelligence cycle comes in for criticism, especially in the national security space. In this regard, one of the more studied documents is A. S. Hulnick's (2006) piece entitled "What's Wrong with the Intelligence Cycle." Hulnick, previously an analyst with the CIA, notes that one of the main flaws is that policy makers tend to frame requirements that support their views, rather than being informed by the intelligence they receive. Although obviously more prevalent in the national security space, this is also common in businesses. Hulnick also considers that the cycle misses two critical functions—counterintelligence and covert operations—although these are of less obvious relevance to corporate interests.

A more common claim is that the cycle is an overly simple representation, especially in the current age, where availability and access to information is expanding so rapidly, and where threats are more networked and connected, especially in the terrorism and organized-crime environments. Analysts are increasingly finding that the information they need is already available within the mass of collated data available to them, and consumers and decision makers are digging into product on more

of a pull than a push basis. Furthermore, the speed at which things are required means that a linear process may slow things down unduly. This all points toward a flatter, more coherent structure whereby functions work within a network to develop shared understanding. This is the basis of what is called the *target-centric approach*, first advocated by Robert Clark (2003) (Over ten years on, his book *Intelligence Analysis: A Target-Centric Approach* is now in its fourth edition, showing the continued interest in his thinking.)

This evolution in approach is also being driven by the competing needs of what Sir David Omand (2010) recognizes as "action-on" intelligence, versus more strategic situational awareness. Reacting quickly not only requires constant knowledge of the environment and the ability to spot critical items of intelligence, but also thorough understanding of the customers' needs. This is particularly pertinent in the corporate sector, where time is money and relevance of information pure gold, and where bureaucracy is becoming increasingly unpopular. Sir David, in his book *Securing the State* (2010), proposes a modified "National Security" All-Risks Intelligence Cycle, which combines elements of both the traditional approach with the more modern idea of a networked function. The key aspect of this is that rather than feeding in at the Direction stage and then feeding back as part of Evaluation, the consumer sits in the middle of the circle. This gives them visibility of the process and access to information at all stages—a most desirable outcome. (Note that Sir David also removes the traditional names for the different phases, again underscoring his own desire for a transition away from the older models.)

A Suggested Model for the Corporate Security Intelligence Cycle

With all of these considerations in mind, our suggested corporate security intelligence cycle is broken out in Figure 5.4. This forms the basis for the next few chapters and is the underlying core of the Security Intelligence Decision Advantage Research Model (SIDeARM), a best-practice, off-the-shelf tool for implementing an effective corporate intelligence process (discussed in detail in Section III of this book). As can be seen, it adopts something of Sir David Omand's (2010) approach. However the difference is that the there is a function of both client and process management in the center. This is the hub of the wheel, and an axle (or driveshaft if you prefer to think of the wheel as a motor!) connects this to the clients.

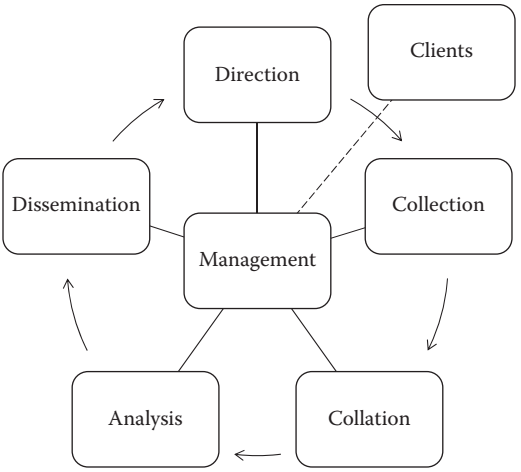

Figure 5.4 Our version of the intelligence cycle.

In the corporate environment, this approach is suggested for several reasons:

- Senior corporate clients are highly time sensitive and are more inclined to let things operate with autonomy.
- In modern business, influence is based strongly on people's personal relationships rather than hierarchy or even process.
- Uncontrolled client access to analysts would result in significant drags on time and efficiency.
- Conversely, uncontrolled analyst access to clients could not only impact time, but also result in confusion and policy paralysis.
- Too flat and networked an approach enables bad practices such as everyone "honey-potting" onto the tasks they are most interested in, or dealing with the current crisis at the cost of spotting the next emerging threat.

Under this model, it is very much the manager's role to think like the client and anticipate their needs while maintaining constant oversight of the intelligence process in a fashion that clients would not possibly be able to. Obviously, it relies heavily on the seniority, interpersonal skills, and judgment of the manager sitting in the center, who not only has to handle clients, but must also arbitrate issues within the team, especially in terms of resource allocation. In practice, though, this is a highly efficient

arrangement, keeping the discipline of the linear process while allowing all the benefits of networked approaches to the task.

PRINCIPLES OF INTELLIGENCE: CROSSCAT

Western military thinking identifies eight principles of intelligence. The military likes to present things in a way that can be recalled well under pressure, and so likes to use mnemonics—in this case CROSSCAT. This stands for the following:

C: Centralized control
R: Responsiveness
O: Objectivity
S: Systematic exploitation
S: Source protection
C: Continuous review
A: Accessibility
T: Timeliness

In more detail, these are as follows:

Centralized control: Essential to avoid duplication of effort, to provide mutual support, and to ensure efficient, economic use of all resources. In a large group of companies, there should be a single authority at the highest level in which intelligence is used within the group. Thus if several companies in the group each have an autonomous intelligence function, the single focal point should sit above them at group level. However, if a single business unit is unique within the group, then the single focal point for intelligence should sit at leadership level.

Responsiveness: Security intelligence operators and managers must remain alert to the changing information requirements of decision makers. These are driven by changes in markets, business strategy, financial strength, or even something as simple as a new appointment to a senior leadership position.

Objectivity: Any temptation to distort information to fit preconceived ideas must be strongly resisted. Some analysts will have a natural bias based on beliefs, experience, or corporate attitudes. It is essential that analysis remain as unbiased and objective as possible.

Systematic exploitation: Sources and agencies must be systematically exploited by methodical planning, based on thorough knowledge of their capabilities and limitations. In this way, collection will be optimized and the most reliable and productive sources tasked; moreover, sources will not be missed or overly stressed (in the case of human sources; see Chapter 7, Intelligence Collection). Tasking should be managed according to priorities determined by the intelligence manager in consultation with senior managers.

Source protection: All sources of information must be adequately protected to preserve their ability to generate raw data and mitigate any threats they may face themselves. Source protection is a complex issue that goes beyond simply not naming sources or people; it is often amazing how much a report can reveal about the organization asking for it. A simple distribution error can lead to a compromise that—in some environments—might even have fatal consequences.

Continuous review: Intelligence forecasts must be continuously reviewed and, where necessary, revised, taking into account all new information. All involved should constantly ask themselves: "Does this change the current assessment?"

Accessibility: Intelligence is of little value if it is not disseminated to the user. All relevant intelligence must be made available to decision makers, and this imperative ties into the push-versus-pull debate outlined here.

Timeliness: Intelligence is largely useless if it arrives too late. Intelligence must be judged as to its perishability by the intelligence manager. In a fast-moving situation, it might be necessary to simply telephone a message to a key individual to alert them to some highly time-sensitive intelligence. (However, in such circumstances, it is still advisable to send a fully analyzed and formatted report as a follow-up confirmation and for the purposes of knowledge management.) Intelligence must be tailored to the requirements of the user, provided in a useful and comprehensible format, and received in time to affect the decision-making process. Delivery of the right intelligence—not simply data or information—to the right place at the right time is the guiding principle of all dissemination efforts.

As with all guiding principles, these often create tensions that are slavishly adhered to. For example, there is a clear need for judgment to balance between accessibility and source protection. This is perhaps best

highlighted by then-PFC Bradley Manning's release of classified diplomatic information, which he was able to obtain due to the US military deciding to make things as accessible as possible. Such conflicts are inevitable, and it is the role of key personalities within the team to handle these conflicts.

DRAMATIS PERSONA: ROLES AND RESPONSIBILITIES

This is a good time to talk about the personalities within the corporate intelligence process. The main roles are as follows:

- Intelligence manager
- Collector
- Collator
- Analyst
- Administrator
- Consumer (or client)

These functions are quite discrete and often require very different skill sets. Unfortunately, many organizations will not have the resource budget to enable all of these posts. Instead, those with responsibility for intelligence must get used to wearing a lot of different hats! Even in this case, understanding of the theory will help to produce better results, since one can then think appropriately when undertaking certain stages of work. It is therefore worth addressing each role in turn, as follows.

Intelligence Manager

The intelligence manager has overall responsibility for coordination of the team and output of the product. This role is therefore central to producing high-quality material. In our suggested model, the intelligence manager sits in the center of the team's activities and is responsible for monitoring resources, coordinating actions, and ensuring that everything works in harmony. They often spot efficiencies and synergies, and they juggle between tasks in order to meet client needs as best as possible. They are also generally responsible for interpreting clients' needs and transforming these into actions and outputs, acting as a surrogate client for the team when advising on what is of importance or of relevance.

The intelligence manager is therefore likely to have high project management skills and be able to run a team efficiently, prioritizing

and distributing work and constantly assessing processes. They should also have the ability to see the "unknown unknowns," so this is not a process-oriented task. Rather, this is a very senior position, and the role is best suited to someone with significant experience and knowledge of what the clients need. They must also be prepared to serve as a mentor and advisor to all members of the team, and in the corporate environment will often, although not always, have served time in an analytical role. Other qualifications include high written and verbal briefing skills.

An important point, often missed, is that this is really a *leadership* position as much as a management one. Intelligence work can involve great stress and intense deadlines, plus exposure to undesirable people, images, and other material. Crises always seem to break at the least convenient times, and people may often be confronted by the unexpected. Moreover, some roles can demand relentless cycles of shift work, and intelligence is more often in the headlines for getting it wrong than for getting it right, which can sometimes make forecasting a grueling and thankless task. Helping keep a team's morale high is therefore one of the key factors of the intelligence manager's role, with the provision of vision and a clear purpose being the very least that can be expected.

Collectors

Collectors are responsible for bringing in data and information. They may sometimes be called *operators* (a more national security-oriented term) or *researchers* (more corporate friendly). They tend to be specialists in a certain area, for example human or geospatial intelligence. Their skills are often technical, and a good collector may not always make a good analyst (and vice versa), although in some smaller setups, the same person may undertake both roles. In a corporation, most intelligence collection is via open sources (OSINT; see Chapter 7), and so the majority of collectors are employed in this field. Their role is fundamentally to bring in everything that might be of relevance to the organization, based on what they have been directed to do by the intelligence manager and what they know of the environment. Collectors are therefore most effective if they are fully aware of the wider needs of their clients, although this is a step that is sometimes problematic.

In an ideal world, everyone in the security function of the organization would probably be trained as a collector, although in practice this is difficult to achieve in a formalized fashion.

Collators

Collation is often undertaken by collectors or analysts; it is rarer to have this as a discrete function. However, it is vital, as discussed previously. Individuals in this role must have a "tidy" mindset, as their main function is to store and catalog data in such a way that it can be immediately useful to analysts. It is helpful for collators to have knowledge of geospatial (GIS) tools, databases, and spreadsheets. Since collators are often responsible for initially spotting patterns in data, they generally progress to be good analysts and can very useful in identifying unusual trends and events.

Analysts

Analysts are seen as adding the most value to data. Indeed, there is a strong argument that many intelligence failures are due to analysis rather than collection. (It is therefore interesting that many countries spend well over 90% of their national intelligence budgets on collection activities rather than analysis.) An analyst is the most likely dedicated intelligence post to be found in a corporate organization. Despite this, the general approach to analysis remains poorly understood. Not too long ago, people were picked for subject-matter expertise and left to run loose. Analysts have therefore tended to lean heavily on academic training, but since the 1980s, this has gradually changed, at least in the United States. An analyst is best seen as being an "extroverted introvert" (or outgoing thinker), a difficult combination to master. The analyst's brain is ultimately one of the most important single items in the intelligence apparatus. Indeed, as often discussed in this work, attempting to remove humans from the process is one of the great traps of today's environment. We will therefore examine the desirable psychology, skill sets, and approach of an analyst in more detail in Chapter 9.

Administrators

Administrators are a rare luxury. They obviously help support the organization of the team, especially in regard to resource management, and they support the intelligence manager (who, after all, has responsibilities such as client management and quality control to work on). However, they can also be very useful in the process, for example in terms of updating a website or sending out reports. There are also organizations where the administrators proofread all reports from a client point of view, which

works well, as they have not formally been involved in the rest of the process. Remember that intelligence is a constant battle to get the most out of the assets available, so do not underestimate what the administrator can potentially bring to the party. If an analyst can save thirty minutes uploading reports and instead spend time horizon scanning, that will ultimately be to the benefit of the process as a whole.

Consumers

Consumers—or clients—are generally the decision makers in the organization. This can be at all levels. For example, all staff ultimately rely on travel-security intelligence when going about their business, or they need general context around their security awareness. Many people may not consider them a part of the intelligence team/process, but they most certainly are. The best consumers are those who fully understand what they are getting and who have a say in why it is being produced (the "how" is less desirable, as this can result in micromanagement of the intelligence team). Their involvement in the process is therefore critical, especially in the corporate environment, where budgets are not guaranteed and much depends on effectiveness of output.

Ultimately, the key measure of a successful relationship is getting your consumers to proactively communicate their needs and any other feedback. This comes through trust and obtaining buy-in, which is a gradual process. This is one of the hardest parts of positioning an intelligence function. In the early days, there is generally a tension between getting decision makers to take notice and then preventing them from overloading the system or placing too much faith in it. Again, trust and regular, friendly communication with consumers—often informal—does much to set up an efficient operation. The process of education is key and relies greatly on the "soft power" of the intelligence team's representative (in our model, the intelligence manager). Of course, buy-in also relies on the quality of the decision advantage the team can offer the consumer, so there is a cycle of improvement here. Moreover, the education process can often be two-way: The intelligence team needs to understand the business of the decision makers in order best to support them.

Top-level sponsorship, usually from senior consumers, is a huge boon in winning a role within the organization as a whole. This usually relies on the function being seen as an enabler, or at least a critical and cost-efficient defense, drawing heavily on the measures and topics

introduced in Section 1 of this book. Given the rapidly changing corporate environment, the business of finding and maintaining sponsors and influential consumers is thus an ongoing effort, worthy of considerable attention. The ultimate success measure is becoming firmly enshrined in business processes, which both clarifies and cements the role of intelligence in the enterprise—and hopefully improves safety and security for all.

TYPES OF INTELLIGENCE

Intelligence can be categorized into various different types. Note that these are not the same as the types of intelligence people from a national security background that you may immediately think of, for example open-source intelligence (OSINT) or human intelligence (HUMINT). Those terms relate to *sources* of intelligence and are discussed in more detail in Chapter 7, which covers intelligence collection. Instead, we are talking about categorizations of purpose, as follows:

Current intelligence addresses day-to-day events and seeks to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potential dangerous situations in the near future.

Estimative intelligence deals with what might come to pass. Its main role is to help decision makers navigate the gaps between available facts by suggesting alternative patterns into which those facts might fit and to provide informed assessments of the range and likelihood of possible outcomes.

Warning intelligence sounds an alarm or gives notice to decision makers. It includes identifying or forecasting events that could trigger the deployment of immediate countermeasures or those that would have a sudden and deleterious effect on the corporate position. Warning intelligence often also involves exploring alternative futures and low-probability/high-impact scenarios.

Research intelligence consists of in-depth studies. It underpins both current and estimative intelligence. It primarily consists of the structured compilation of geographic, demographic, socioeconomic, security, and political data on operating environments. It also includes the drawdown of material to help support operational decision making.

These types matter, as they can often define the approach to a task. Moreover, they can aid greatly when trying to work out how best to address a client requirement. Sometimes all types will apply even when covering a single issue.

THE SYSTEMS APPROACH

The world is a complex place, and it seems to be getting more so by the day. The challenges outlined in Chapter 2 indicate that this is not likely to change soon. Dealing with complexity is a major challenge to an intelligence team. The systems approach is therefore very useful. As briefly touched upon several times already, the systems or network approach lies at the base of adopting target-centric analysis, and this approach has gained great currency since 2000. In its publication *Joint Intelligence Preparation of the Operational Environment*, the US military defines a system as an "interconnected or interrelated network, group, or chain—a functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole."

The systems approach is heavily used to understand complex problems; for example, systems engineering was an approach developed by NASA when designing the space shuttle orbiter. This visualized components as part of systems, and systems as part of "systems of systems." Take for example a car; this can be viewed as a system made up of subsystems, e.g., the engine, the braking assemblies, the steering, the climate control, and so on. Systems engineering works on the basis that a system may work perfectly well as designed, but when integrated with other systems, unexpected problems can emerge due to complexity. These are called *emergent factors*. Pursuing the example presented here, the engine may work fine on a test rig, but when integrated with the chassis of a proposed new design, which also works fine on its own, a vibration problem ensues.

How is this relevant to intelligence? Well, the reality is that many things are systems. Criminal groups form systems within their environment, and geopolitical affairs often manifest emerging factors that can lead to unexpected surprises, to take just two examples. Mapping the known relationships can sometimes allow us to understand potential issues arising from a course of action and better understand the context and rationale of events. This can even help us spot emerging threats, allowing preemptive mitigation—which should be the ultimate goal of any intelligence apparatus.

We generally portray a system as a network, with two main parts:

- *Nodes*: Events, people, or things
- *Links*: The connections between the nodes (also sometimes known as *edges*)

Links can sometimes be *directional* in order to show influence. This can particularly help in showing potential issues arising from changes in the system (e.g., if a key player is removed from a criminal network, or if a global incident were to drive up oil prices). An infamous example was a slide produced by PA Consulting Group in relation to the conflict in Afghanistan. Although hailed by detractors as the epitome of "PowerPoint warfare," the slide actually does a very good job of portraying the complexity of the system. It certainly shows that there are no easy answers to complex problems! On a similar note, one of the issues that can affect analysts is oversimplifying the system in an effort to understand it. This is the other extreme of PowerPoint warfare, where decision makers are presented with concept diagrams that have stripped away too much complexity. This serves the decision maker no better than the more complex approach, and may in fact be more dangerous, as a false sense of security and understanding can be generated (a major problem with many risk-management approaches, in fact).

In sum, the systems approach is a way to help deal with complexity, but not necessarily by simplifying it at the cost of granularity and nuance. As it is such a core factor, examples of network and systems approaches will be discussed in more detail in Chapter 9, which covers analysis.

PREDICTING, FORECASTING, AND PROBABILITY

Although not strictly a theoretical point, discussion of complex systems makes this a good point at which to clarify one of the key misconceptions about intelligence. As previously discussed, intelligence involves dealing with uncertainty; this is unavoidable, and all of the approaches outlined in this book represent attempts to try to gain understanding and insight. What we cannot do is predict the future; instead, intelligence is built around forecasting. The best analogy (in many ways) is the weather. Even with hugely complex and well-researched models, a multitude of sensors, and huge computing power, weather forecasters still fail to be accurate. This is partly because of the huge amount of variables at play and our imperfect

knowledge. As models and understanding improve, we are getting more and more accurate, but the weather can still take us by surprise.

As with so many weather forecasts, we therefore use *probability* to express our confidence in the outcomes of imagined scenarios. This is often expressed as a percentage, although a standard of language has also been developed that allows confidence to be expressed in a more natural way (through the use of terms such as *likely*, *probable*, and so on). We will come back to this and provide a useful guide to such language in Chapter 10, which talks about writing and reporting for intelligence consumers.

CONCLUSION: ALL PARTS IN A HARMONIOUS WHOLE

This chapter has served as an introduction to the top-level theory underscoring intelligence operations. The key points are as follows:

- Information is not intelligence. Rather, data needs to be converted into insight through a rigorous structure that brings together people, process, and technology to best effect.
- The intelligence cycle forms the basic underlying framework for effective intelligence operations. The debate over what exact form it should take should not distract practitioners from embracing and fully understanding the process.
- Critical features include: the management of all resources to achieve the most efficient output; the careful definition of intelligence requirements; the collection of material in the context of a defined and structured collection plan; the effective management of knowledge; and the involvement of a finely tuned, analytical human brain in the process.
- Success is impossible without the education and involvement of business decision makers, and this can be facilitated by using the arguments outlined earlier in this book.

Learning from mistakes is at the heart of the intelligence business, and those that cannot handle failure and criticism need not apply. Ultimately, trying to make sense of partial data is maddening, and self-criticism is therefore highly important. It is worth concluding by offering some discussion of common failures and pitfalls.

- Inefficient knowledge management resulting in missed opportunities, usually in the form of missing connections

- Lack of focus on decision makers' needs in favor of what the analyst/team were more interested in (known as *producer capture*) (This can include presentation of material in unsuitable formats as well as being off target on defining requirements.)
- Inefficiencies, confusion, and stress resulting from insufficient management and leadership
- Missing, inaccurate, or unduly biased data due to the lack of a rigorous collection plan
- Overreliance on "hard" or "positional" power instead of attempting to extend influence and build relationships
- Failure to influence decision makers by not being involved in corporate processes, e.g., risk structures or compliance frameworks
- Being seen as an impediment to operations rather than an enabler

These pitfalls are common to all intelligence operations, but the private sector is particularly vulnerable to withdrawal of budgeting resulting from these failures. While public-sector-funded intelligence organizations most certainly worry about budgetary issues, the prospect of continually fighting for survival is not terribly urgent. (For example, while the CIA and other agencies may compete for influence and a degree of funding, they are unlikely to be cut altogether, and if they fail, they may even benefit through enhanced funding.) This is because the "client" for national agencies is usually already convinced of the need for intelligence, something that is sadly still not the case in the majority of corporate entities, although this is steadily changing. Therefore, the need to maintain relevance through focusing on clients cannot be overstated, meaning that the intelligence machine has to run at optimum pitch all the time. Understanding and applying the basic theory here will go a long way toward making the apparatus as effective as possible, maximizing the chances of success.

6

Management and Direction

> It is impossible to provide a forecast of future contingencies, especially because on our expeditions we are obliged to go across great waters and vast solitudes by dangerous ways…on account of which they frequently depend on God's will and disposition, and of course the weather.
>
> **The Grand Master of the Teutonic Knights, 1394**

CHAPTER OBJECTIVES

1. To explain how intelligence requirements are derived, articulated, energized, and actively managed.
2. To underscore the importance of managing an intelligence process in as efficient a manner as possible.
3. To discuss the concept of knowledge management within a corporate intelligence environment.

INTRODUCTION

The previous chapters have discussed the principles and theory of intelligence. Many of the points raised have emphasized the importance of capable management in order to help combat uncertainty. This includes the need to manage people, processes, time, quality, sources, partners, clients, and knowledge across the enterprise—a demanding task.

This chapter therefore looks in detail at the role of management. Unlike the subsequent chapters, which focus on things more easily recognized as "stages" in the intelligence cycle (e.g., collection), this cuts across all aspects of the intelligence effort. We will therefore break this down as follows:

- Defining, articulating, and energizing intelligence requirements (IRs)
- Managing people and processes
- Managing clients
- Knowledge management

THE "THIRTEEN RULES"

The "Thirteen Rules" were written by Admiral Sir John Godfrey RN, who served as the UK's director of naval intelligence from 1939 to 1943. He was an interesting and capable character, and Ian Fleming, the naval intelligence officer turned writer, used him as the model for "M" in the James Bond series. His tongue-in-cheek manner shows up clearly in the following list; his willingness to fight in his corner eventually resulted in him being promoted sideways. Nonetheless, these rules are his legacy as a highly capable manager of an intelligence function, and with little effort many can be used as guidelines for the modern corporate security intelligence manager.

1. Fighting commanders, technical experts and political leaders are liable to ignore, under-rate or even despise intelligence. Obsession and bias often begin at the top.
2. Intelligence for the fighting services should be directed as far as possible by civilians.
3. Intelligence is the voice of conscience to a [military executive] staff. Wishful thinking is the original sin of men of power.
4. Intelligence judgments must be kept constantly under review and revision. Nothing must be taken for granted either in premises or deduction.
5. Intelligence departments must be fully informed about operations and plans, but operations and plans must not be dominated by the facts and views of intelligence. Intelligence is the servant and not the master.

6. Reliance on one source is dangerous; the more reliable and comprehensive the source, the greater the dangers.
7. One's communications are always in danger; the enemy is always listening in, even if he cannot understand. Intelligence has a high responsibility for security.
8. The intelligence worker must be prepared for villainy; integrity in handling of facts has to be reconciled with the unethical way they have been collected.
9. Intelligence is ineffective without showmanship in presentation and argument.
10. The boss, whoever he is, cannot know best and should not claim that he does.
11. Intelligence is indivisible. In its wartime practice the divisions imposed by separate services and departments broke down.
12. Excessive secrecy can make intelligence ineffective.
13. Intelligence is produced from files, but by people. They require recognition, continuity, and tradition, like a ship or a regiment.

Managers do particularly well to remember points 10 and 13!

INTELLIGENCE REQUIREMENTS AND PRODUCT DEFINITION

As we have seen, intelligence requirements (IRs) are what really make the intelligence cycle rev away—the fuel for the engine, if you will. Like an engine, the quality and quantity of fuel make a difference to output (including the risk of flooding if there is too much)! The articulation of IRs is therefore one of the most important aspects of the whole intelligence process in a company. Amazingly, this also seems to be one of the areas that is most often neglected. It is a rare corporate security department that can clearly explain and elucidate what it needs to know. Although there is often some agreement on a general idea, the specifics are missing. In part this is due to "business as usual" and the phenomenon of firefighting rather than being able to take a strategic step back and consider the needs of the business.

IRs have characteristics as follows. Ideally, each should:

- Ask only one question.
- Focus on specific facts, events, or activities concerning an adversarial element or the security operating environment.
- Tie to planning, decision making, and execution.
- Provide a clear, concise statement of what intelligence is required.
- Contain finite temporal or geographic statements to limit the scope of the requirement.

A simple IR may therefore be as follows:

> What is the probability of al-Shabaab launching attacks threatening our corporate activities in East Africa during 2014?

In the ideal world, a consumer of intelligence would issue perfectly articulated IRs to the intelligence team. This can be seen in the military, but rarely elsewhere, even in the public sector. Instead, it is more common for the intelligence manager to have to interpret client requirements and translate these into action.

The aim is for IRs to set out a clear scope of work that can be used to inform the collection plan and analytical process to help provide an effective product back to the client. In practice, many IRs may be included within a particular product; for example, a routine country-risk report could cover a wide range of topics that are of relevance to the business. In this case, although the product is more complex, the IRs themselves—when broken down—remain as simple as possible.

This hints at a common error, which is to make IRs too broad. Specificity helps to break down a complex problem—which, as we've discussed, is the nature of intelligence work. Breaking down the problem helps provide more focused requirements to the collectors and analysts, and this can be a significant aid to clarity throughout the process. Equally, analysts and collectors should themselves be involved in creating their own requirements, which is in part something that comes as a natural part of hypothesis testing within the analytical process (see Chapter 9 for more on this).

A useful trick when breaking down complex tasks is to use top-level IRs in combination with subheadings. To take the project-based example presented here a step further:

IR 1. What is the probability of al-Shabaab launching attacks threatening our corporate activities in East Africa during 2014?

IR 1.1. Where are we operating, or otherwise have business exposure (e.g., supply chains) in the region in question?
IR 1.2. What is the current intent of al-Shabaab's leadership?
IR 1.3. What have been al-Shabaab's previous activities in the countries in question?
IR 1.4. What capabilities does the group currently have?
IR 1.5. Which allies might they call on?
IR 1.6. What other factors may impact their capability in 2014?
IR 1.6.1. UN action in Somalia
IR 1.6.2. Activities by nations surrounding Somalia

Often, if managed correctly, the elucidation of IRs can also act as a form of "contract" with the client, especially for project-based work, although this also works for routine tasks. An initial assessment and breakdown of the task can be presented as a list of IRs to be addressed. This can be combined with a description of context, a list of resource requirements, a suggested timeline, and a definition of the product/deliverable in order to provide a simple, condensed, and effective outline of the task in its entirety.

The plethora of IRs being generated means that there is a need to effectively keep track through a dedicated process (most commonly a spreadsheet, although more complex systems can be used where appropriate). Effective management of IRs also includes the identification of priority requirements, sometimes formalized as PIRs. These are the more important or urgent tasks, often established in combination with senior clients or security practitioners. Identifying PIRs helps collectors and analysts make decisions when managing their own workload, and it helps focus the team—although potentially at a cost of missing something important developing elsewhere, as is always the case in intelligence work (too much to do and never enough time, resources, or access to knowledge).

The other part of effective management consists of realizing where to harmonize or group IRs. This can help to streamline collection and the development of suitable products. For example, a country-risk report for numerous recipients within a business could usefully cover all of their requirements, grouped by geography, with these IRs being used to provide indications of the appropriate headings within a report. When servicing multiple clients, this approach is also particularly useful, as it can allow for a piece of work or analysis to be repeated in a format or collection that is of most use to the reader. This again helps to make the setup more efficient, meaning that resources can be spread further and output improved.

How to derive IRs is probably the question the author has been asked most often when discussing intelligence with peers and clients. There are of course many techniques. However, this is basically a function of clients/consumers putting enough time aside to think strategically about their needs. The manager can help this by working regularly with the clients to understand their needs and then translate these into actions for approval. The key is to maintain this involvement, ideally through routine meetings. This serves as a reminder of how IRs should, as a whole, be reviewed and updated regularly inside the intelligence function. Again, this is a vital function of the manager.

Ultimately, IRs are the lifeblood of the entire process and, as such, must be kept *clear*, *current*, and be amply *communicated*. This is the manager's key responsibility and is a vital part (in our model) of how the manager's role as a client-focused directing hub for the activities of the intelligence team. This also incorporates a process of gaining feedback on the team's performance; have IRs been met? Are products adequate for the task? And are there more that can be added? These are questions that should be addressed often. In this regard, there is little to beat face-to-face feedback, although other methods of quality assurance have been deployed successfully, for example in the form of questionnaires and even "like" or "comment" buttons on e-mails. These will be addressed in more detail in later chapters.

MANAGING PEOPLE AND PROCESSES

The manager is also responsible for much more than just the handling of client liaison, however. As Admiral Sir John Godfrey said in his 13 Rules, intelligence (as with so much in life) is ultimately about people. The modern obsession with technology should not be allowed to cloud this salient fact. Almost all intelligence jobs are endlessly demanding, not least because of the severe challenges in constantly battling a lack of certainty and so often being wrong. Discipline and rigor do not come easily and cannot be taken for granted, requiring firm leadership and the setting of high standards. This must be tempered with compassion; topics often break "out of hours," and surprises are almost always bad. As previously discussed, failures inevitably draw more attention than successes, and being prepared to accept and learn from these requires a serious change in mindset. Again, the vision and support must come from the top—a function of leadership more than management.

What keeps the team motivated through all this is a sense of the real value and worth in what they are doing. The leader is therefore responsible for making sure that all work is valued and effective, and that the team knows this. They particularly need to know that they have management support to bring potentially contentious views to the table, and that they will be given a fair hearing. In fact, the principle of fairness is very important throughout, helping to build a team culture whereby people know that they can share ideas freely, and yet have a clearly defined "place" in things and sense of responsibility. Ownership of particular products is a great way to enable this, making people feel like more than just a cog in a wheel. Equally, client exposure should be enabled for the collectors and analysts.

Ultimately, the sense of involvement and shared purpose among the team, coupled with the considered sharing of thoughts and ideas, is of great value in making the engine run as smoothly as possible. Aids to this include a well-promulgated *mission* and *vision statement*, both of which should be signed off by senior management. The sharing of results with the team is also of the utmost importance, and again, this is all too often overlooked. However high someone's initial dedication to the task, should they then find themselves to be part of a sausage machine firing off analysis into the ether without any tangible effect, their efforts will soon fade.

Regular staff reviews are of course also a priority. These will usually be mandated by the human resources (HR) policies of the ultimate employer. However, this is not to say that these policies are enough. Analysts in particular are highly motivated by achieving effect, and the best are therefore continuously seeking feedback. This goes hand in hand with maintaining discipline and rigor in analysis. Constant criticism sounds negative, but the best operators soon realize that this is a business of minimizing imperfection (a little like wars being won by the least disorganized side). The leader needs to communicate this and maintain morale while still constantly challenging, testing and, yes, criticizing the team—a difficult balance, but essential. A useful parallel here is the best newsrooms—a high-pressure, demanding environment with few rewards other than the immense satisfaction of a job well done…and then the cycle begins again. Pay is low and the hours stink, and yet people queue for these jobs, for the chance to make a difference.

From this discussion, "firm but fair" is probably the main overriding theme. It is also essential for managers to share their own experience while also acknowledging their limitations. Delegation is key to success, however tempting it may on occasion be for experienced managers to just produce something themselves; after all, the more that can be imparted

to the team, the more capable they become. This is not a zero-sum game; given the almost limitless nature of the task, the intelligence apparatus can continuously improve its output both in terms of quantity and quality. Investment in people reaps rewards.

Of course, even the best people infused with a great mission and values can fall flat on their face without the guidelines and structure to harmonize their efforts. We are all aware of sports teams made up of individual superstars, yet which lose games to technically less worthy opponents who play better as a team. Similarly, what is required here is a balance between individual artistry (leadership of people) and science (management of processes). We have discussed how intelligence is itself the output of a disciplined process, which is essential to make properly balanced assessments of uncertainty. The intelligence cycle, or a variation thereof, is the minimum structure required (whatever the quibbles with its exact form). However, there is much more that can really help things hum along nicely. Key things to consider are *standard operating procedures* (SOPs). These lay down the various ways in which anticipated tasks will happen. SOPs avoid confusion, drive efficiency, enable people to understand the boundaries within which they can operate freely (thereby improving the range and quality of outputs), and minimize the pressure on the manager/leader to constantly micromanage the team. They are therefore well worth the investment in time and effort, acting in effect as the lubricating oil for the intelligence engine.

A rather comprehensive list of examples of SOPs is offered in the accompanying sidebar. However, some key things to consider within your SOPs include the following:

- *Working routine*: The military calls this *battle rhythm*. Again, this helps ensure that things run smoothly, particularly out of hours (which is of course when everything seems to happen, and when the most can go wrong).
- *Templates*: Having standard templates helps drive uniformity of product, which is professional and drives up client confidence in the intelligence output.
- *Direction on standards*: This can include guidance on spelling conventions, transliteration, dates, naming of documents, and so on. As readers may already appreciate, this is particularly essential with regard to harmonizing the collection of data and knowledge—something discussed in more detail later in this chapter.

STANDARD OPERATING PROCEDURES

The full list of SOPs in the largest and most complex organizations can be rather extensive. The following is just one example. Of course this is not definitive, and what matters is that the SOPs are appropriate to your organization; there is no standard template. Instead, this is one of the areas where it is worth investing constant effort.

General SOPs
- SOP 1 Concept of Operations
- SOP 2 Daily/Weekly Routine

Security, HSE
- SOP 3 Standing Security Instruction
- SOP 4 Access Control Guideline—Analysis Center
- SOP 5 Emergency Response Procedures—Analysis Intelligence Center
- SOP 5A HSE Instruction

Direction
- SOP 6 Management Guide to Directing Intelligence Operations
- SOP 7 Guide to Information Requirements Management
- SOP 8 Requests for Information Submission Template

Collection
- SOP 9 Collection Management Guide
- SOP 10 Collection Plan Template
- SOP 11 Source Category List
- SOP 12 Human Source Handling Guide
- SOP 13 Human Source Register Template
- SOP 14 Source Handling Procedures Flowchart
- SOP 15 Source Handling Form 1—Pre Meeting Procedures
- SOP 16 Source Handling Form 2—Post Meeting Procedures
- SOP 17 Open Source Intelligence Guide
- SOP 18 Interviewing Strategies
- SOP 19 Generic Security Information Reporting Form

Collation
- SOP 20 Information Flow

Processing (Collation/Analysis)
- SOP 21 Basic Analytical Guidelines
- SOP 22 Incident Database Template

- SOP 23 Personalities Database Template
- SOP 24 Database Entry Guide
- SOP 25 Information Grading Guide
- SOP 26 Classification Guide

Dissemination

- SOP 27 Reporting Parameters
- SOP 28 Product List and Descriptions
- SOP 29 Report Writing—Style Guide
- SOP 29A Report Writing—Sanitization Guide
- SOP 30 Early Warning Report Template
- SOP 31 Information Report Template
- SOP 32 Incident Summary Template
- SOP 33 Assessment Paper Template
- SOP 34 SMS Hot Tipoff Template
- SOP 35 Product Distribution Matrix
- SOP 36 Website Template
- SOP 37 Guide to Updating Website

Business Controls and Systems

- SOP 38 Value for Money Estimation Process
- SOP 39 Task Management Plan Worksheet Template

Business Integration

- SOP 40 Support to Asset Protection—Threat Assessment Template
- SOP 41 Support to Emergency Response Teams
- SOP 42 Support to Corporate Communications
- SOP 43 Support to Community Liaison
- SOP 44 Support to Legal Affairs
- SOP 45 Corporate Security Feedback Loop
- SOP 46 Security Operating Levels—Guide

Miscellaneous

- SOP 47 Definitions for Use in Intelligence Analysis and Reporting

Of course this many SOPs may be hard to digest. At this point, it is worth recalling that to be effective, SOPs must be simple enough to be read, understood, and kept "alive." To this end, it is best for them to be readily available (noting the sensitivities of some items!), ideally on SharePoint or any other sort of flexible platform.

- *Analytical process steps*: This can be as basic as having a "four eyes" policy, whereby no written output leaves the team without being checked by at least one other person. At the far end, this can include procedures for detailed scenario-planning sessions and the war-gaming of all hypotheses.
- *Operational security (OpSec)*: The desirability of sharing information freely and breaking silos is countered by the need to maintain security, as suggested by our examination of the principles of intelligence in the previous chapter. Clear guidelines on OpSec are therefore essential. Key items include protective markings on documents and IT/communications security measures. Where possible, these should follow the processes in place across the firm as a whole, and often the role of the SOP is to interpret these into an easily digestible format. Note that the use of militarized terms such as TOP SECRET on documents is generally best avoided in the corporate environment; instead, use the terms appropriate to the organization. This is because these can overly reinforce the negative image of security (see Chapter 1), and also create the potential for a PR disaster should documents leak ("XYZ Bank collects *top secret* information on customers!" etc.).

Another important—and often overlooked—thing is *job descriptions* for each team member. These help to set expectations, especially around standards, and avoid overlap and mission creep between team members. This brings us to one of the most important roles of the manager, which is to avoid *honey-potting*. This describes how people within the team, with the best intentions, may start to focus on what they all consider to be the most attractive/immediate task, rather than maintaining a broad overwatch. They can thus be taken by surprise by those pesky low-probability/high-impact scenarios that are most dreaded (Figure 6.1).

This is the bane even of professional intelligence agencies (albeit this is sometimes as a result of political interference). An example is the case of former US Army Major Nidal Hassan, who opened fire on his colleagues at Fort Hood, Texas. He had become aligned with al-Qaeda's message of radicalization over the Internet. Naturally, the US Army has a unit tasked with countering their enemies' attempts to corrupt their people, including detecting such cases of radicalization (deliberate or inadvertent). Unfortunately, this had been such a rare phenomenon that it seems the unit had, over time, increasingly drifted toward monitoring terrorism and the activities of al-Qaeda as a whole, moving away from its stated mission.

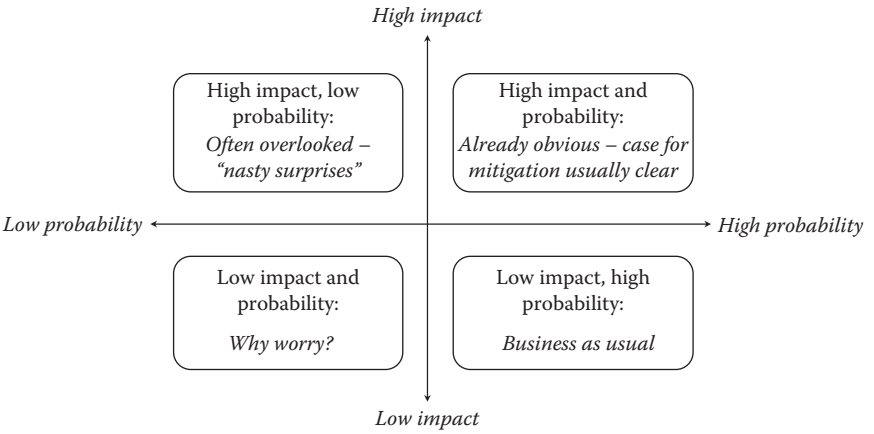

Figure 6.1 Scenarios and impacts.

Their analysis had no doubt been well received by consumers, but it was of course being done (to greater effect) by other parts of the national intelligence apparatus. In fact, a bewildering array of different agencies were focused on this task, and they had already created the problem of "paralysis through analysis," although that is a different story. Regardless, the event that they were established to counter went unnoticed due to the inevitable desire to focus on where the action really seemed to be. This is not to condemn those tasked with this difficult and potentially thankless assignment, but rather to highlight the dangers that can challenge even the best resourced and supported agencies. Again, it is the role of the manager to ensure that all-around observation is being maintained.

This includes one of the most critical aspects of all strategic corporate intelligence work: horizon scanning and blue-sky thinking. As with the case discussed here, the imperative and pressure to focus on the immediate threats and issues can sometimes become overwhelming, but this contributes to the danger of being caught by surprise. The manager in particular must strive to raise the team above the here and now, carving out the time and resources for this vital function.

All in all, the intelligence manager has quite the challenge, and even in the best-run organizations, a lot of time must be spent greasing the wheels. Like the swan, the intelligence team glides smoothly and elegantly above the water thanks to the ceaseless paddling going on below.

MANAGING CLIENTS AND PROMOTING THE ROLE OF INTELLIGENCE IN THE BUSINESS

We discussed the positioning of intelligence in the business extensively throughout Section I of this book. The arguments for utility have therefore already been set out. However, even after the function has been established, the constant mission to maintain business relevance requires the manager to guard against complacency. After all, if you don't like change, you'd probably best get used to irrelevance! The manager of the intelligence function must therefore seek to be both responsive to client needs—no matter how esoteric they may seem—and also proactive in spotting opportunities to further the role of security intelligence, where this benefits the wider enterprise. Ultimately, the winning formula is client satisfaction combined with clear demonstration of value for money to the business. This requires constant attention, forethought, and something of an entrepreneurial streak from the manager, tempered with keen political awareness and a sense of responsibility.

In the variant of the intelligence cycle used in this book, you have seen how we envision the intelligence manager not only as the hub of the intelligence team's activity, but also as a two-way axle/driveshaft to the clients. In other words, he or she represents the clients to the team, and the team to the clients. This overcomes the practical obstructions to the clients having access to material throughout the intelligence cycle, as desirable as that may theoretically be, and also maximizes the relevant guidance to team members. To do this, the manager must be very much in the clients' minds, spending a great deal of time focused on the internal dynamics of the business. Without this sort of persistent effort, the team will be much more reactive, missing out on the many opportunities offered by being proactive—through seeing the issues *likely to be faced* by the business, thereby helping prevent, protect, and prepare for them adequately.

This is of course easier said than done. Much of this comes down to the manager's "soft power," as discussed in the first section of this book. This is an area where, traditionally, the security department can sometimes be more lacking. However, it is the strength of relationships within the business that will enable the manager effectively to operate and win clients over. Time spent understanding them, their needs, and the prerogatives of the business will therefore reap rewards. This also allows for the effective process of education—a two-way street between the intelligence team and the clients, and a constant endeavor.

KNOWLEDGE MANAGEMENT

Much of knowledge management is discussed in Chapter 8, which covers collation. Some readers may therefore wonder if it merits separate analysis here. However, the reality is that effective knowledge management underscores the essence of intelligence activity, as covered in previous chapters. The leader/manager therefore has a significant role in setting the standard, both in terms of structure/process/policy and also by leading through example. This is important, as effective knowledge management requires a boundless degree of discipline and rigor, which does not come easily to most people.

Knowledge management has been recognized as a discipline since 1991, with large companies spending increasing effort in this sphere. The benefits are thus well understood in the corporate environment. This focus, and the relentless march of technology, have both helped to make the manager's job easier. Many firms have effective sharing platforms and metasearch capabilities, and use of assets such as SharePoint help keep track of information and find previous references to a topic.

In some ways, a harder part of knowledge management is therefore the human element—especially in regard to teaching the team to be as diligent as possible in finding references to information internally, rather than focusing on external sources. It is frankly amazing how often analysts will forget to check what has already been prepared and understood on a topic in favor of reinventing the wheel. Effective project management, diligent editing processes, and clear guidance throughout the intelligence cycle will help to enable this, hence my view of the manager as being the intelligence hub at the center of all activity.

Areas to consider include:

- *Ease of sharing information*: For example, making use of internal forms of social media and networking, such as instant messaging programs and other presence software. Forums can also be useful in this regard, especially where they are indexed.
- *Ease of accessing information*: As mentioned previously, platforms such as SharePoint are becoming ubiquitous. These are highly flexible and can be optimized to the task. They allow sharing to be controlled, for example enabling "need to know" in key areas while still allowing for free access to less restricted files. Document libraries can be shared and synchronized with version control and auditing. Continuous site-wide indexing also means that any reference to

a particular name or issue can be discovered in seconds. This allows for very quick linkages between information to be extracted.
- *Ease of updating information*: Features such as wikis mean that information can be continuously updated with ease. Processes can also be embedded to streamline editing and approval of material.
- *Ease of managing complex information*: Databases are a fantastic asset (especially for analyzing "big data"), although these require careful design in order to be effective, as will be discussed in Chapter 8 on collation. Leading the design and strategy for this is a core management function.
- *Ease of learning lessons*: Perfection is impossible in intelligence work. Ensuring that lessons are learned and identified on a systematic basis is therefore vital in order to improve performance. This is often overlooked. After all, it can be painful to examine failure, and there is always other stuff to do. However, vital knowledge can be gained from this process of self-examination, and the feedback needs to be spread around the team in order to maximize the benefit. Mistakes will happen, but making the same one twice is almost certainly avoidable.

Ultimately, given the increasing ease of access to raw information, managing how it is stored and accessed to achieve best effect is more important than ever. While this is made easier by the fact that corporations are already engaging in this area, the manager has a vital role in sorting out the details of how this will be implemented, especially in regard to balancing ease of access with "need to know," source protection, data protection, and other confidentiality issues. These can easily be allowed to overwhelm the intelligence process, so considering these areas early on is a great benefit. Moreover, when under pressure, it is easy for things to slip, and so the manager must continuously audit and assess the effectiveness of knowledge management processes.

CONCLUSION: AN ESSENTIAL JUGGLING ACT

As can be seen from the previous discussion, an intelligence manager has to have a lot of skills. Some desirable traits are as follows:

- Personal leadership
- Time management
- Project management

- Integrity
- Clarity of thought
- High written/verbal communication and presentation abilities
- Political awareness
- Ability to challenge and "crack the whip"

Of course, many others can be derived, and it goes without saying that—like any leader—the intelligence manager should be able to set the example through high personal standards and ability at all roles relevant to the tasks in hand. It is therefore helpful (although not essential) for the manager to have had experience as a collector, analyst, and, ideally, to have sound knowledge of the business. This is particularly important when it comes to translating the requirements of clients into meaningful IRs.

Ultimately, the role of manager is not easy. It is not just ensuring that all parts of the process work effectively, but rather a very holistic role, where the manager is also de facto representing the client to the collectors/analysts and vice versa. Holding all this together, and ensuring that no "blind spots" are being left in the collection and analytical processes, is however of the greatest importance in providing an effective service.

Despite often being overlooked, from the discussion in this chapter it follows that even for a one-man "shop" (or smaller setup), the management role is vital, especially in regard to interpreting needs into a meaningful product. Putting time aside to consider the tasks and subject areas outlined here is therefore well worth the effort, especially if the effort is one day to grow.

7

Intelligence Collection

> War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth.
>
> **Von Clausewitz, *On War***

CHAPTER OBJECTIVES

1. To examine the theoretical underpinnings behind collection activities.
2. To illustrate the drivers for the practice and management of collection.
3. To explain and discuss the different types of sources in the commercial environment.
4. To talk about the validation of information once collected.

INTRODUCTION

Following the Direction stage of the intelligence cycle, Collection is the stage at which relevant data and information is gathered. This information, once properly collated, will move to the Analysis stage to be refined into the finished intelligence product—and hopefully tie up the intelligence requirements (IRs) previously identified. As a result, it plays a critical role in the overall quality of the finished product. It is at this stage that the IRs

must first be translated into concrete action, and any failure to identify and obtain necessary information will have a significant impact further in the cycle. At the same time, gathering too much or nonrelevant, information will also place the collation and analysis stages at a disadvantage before their work has even begun. A comprehensive definition of intelligence collection can therefore be said to be *the timely acquisition of comprehensive, proportional, and relevant information to support the intelligence cycle*.

Intelligence requirements are the key activity fueling the cycle, as previously discussed. It is critical that these are clear, comprehensive, and realistic. When operating under ideal intelligence requirements, the process of collection can be clearly formalized and linear. However, this ideal is not often encountered in the corporate world, and perfectly defined and comprehensive intelligence requirements remain elusive. It is also not uncommon that a client does not understand intelligence in any depth, and may simply give the direction for an intelligence team to "tell me what I need to know." In these circumstances, it is critical to have an understanding of the clients and the particular challenges they face.

Further complicating the collection stage is that even ideal intelligence requirements will still not be able to address what former US Secretary of Defense Donald Rumsfeld famously called the "unknown unknowns," that is to say, information relevant to a client that could not have been considered when the initial requirements and priorities were drawn up.

The complications of imperfect IRs and unknown unknowns place a considerable obligation on the intelligence professional. Not only must they meet the set requirements, but they must also remain alert to other information that could have relevance to the client's interests. The intelligence professional can meet this challenge by maintaining a professional curiosity, a tendency toward lateral thinking, and a general situational awareness that can prompt them to identify and collect relevant information outside the intelligence requirements. While the intelligence requirements should always take precedence, the maxim that intelligence is both an art and a science is relevant here. Collection therefore provides both the foundation and the core ingredients of analysis. Poor quality in this phase will impact the entire process, and thus quality sources of information are critical.

SOURCES

Sources of information in intelligence encompass a wide range, and for ease of administration they have been divided into a number of categories.

As these categories have been developed by military forces and government intelligence agencies, they have been assigned military-styled syllabic abbreviations. They include:

OSINT (Open Source INTelligence): OSINT information is the largest and most important category for intelligence collection in the corporate intelligence environment. The Federal Bureau of Investigation defines OSINT as "a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.)." From a corporate intelligence perspective, we can expand on this definition to arguably include any information available within the public domain, provided access to this information is both legal and ethical.

While open-source information has been utilized by intelligence operatives throughout history, the formal collection of open-source intelligence can be traced back to (a) the widespread adoption of radio for civilian use during the 1920s and 1930s and (b) the US intelligence community's establishment of the Foreign Broadcast Intelligence Service (FBIS) in 1941 to monitor international civilian broadcasts. This service was praised for its output by senior intelligence officials during World War Two as being "the most extensive single source available" on developments in Japan and the Asia Pacific theater. Since the Second World War, the communication and information revolution of recent decades has driven exponential growth in OSINT. Intercontinental phone links, communications satellites, and the PC, the Internet, and mobile phones have increasingly opened up an almost infinite range of information to intelligence researchers. In the majority of corporate intelligence work, OSINT will be the category of the vast majority of information collected.

HUMINT (HUMan INTelligence): Arguably the highest-profile category of information sources is that derived from humans. From the earliest days of organized human warfare, commanders have sought information relating to the disposition of enemy troops in order to gain some advantage. The ancient Greek historian Herodotus recounts the tale of the Persian army defeating Spartan forces at the Battle of Thermopylae in 480 BCE as a result

of information received from a Greek HUMINT source. HUMINT goes beyond information obtained from clandestine sources, however, and can be defined as any information directly obtained from human sources. This includes anything from a conversation with an academic to reading an e-mail from a colleague to attending a conference or lecture. This area will also be the subject of further discussion later in the chapter.

IMINT (IMagery INTelligence): Imagery intelligence is the field of collection that deals with information obtained through satellite and aerial photography. While the use of aerial balloons to observe the battlefield goes at least as far back as the 1861–1865 American Civil War, it was the technical developments in photography and powered flight in the early 1900s that made IMINT a realistic source of information. The First World War was the first major conflict to see the systematic use of aerial photography, while the late 1950s saw the development of reconnaissance (or spy) satellites, which played an extensive role in the Cold War. The cost involved in IMINT has traditionally kept this field for military- and state-level intelligence organizations. However, recent conflicts in Afghanistan and Iraq have demonstrated the use of drones as IMINT sources, and the decreasing cost of drone platforms and the ever-decreasing size of quality digital cameras has the potential to suggest a future role for IMINT in corporate intelligence projects.

SIGINT (SIGnals INTelligence): Signals intelligence deals with obtaining information through the interception of signals. This can include communication between people (known as COMINT) or other electrical signals not used in communication, such as radar or data streams. As with IMINT, the high level of technical investment required to utilize this source category has almost exclusively limited it to military- and state-level intelligence organizations.

TECHINT (TECHnical INTelligence): Technical Intelligence is generally referred to as information about weapons systems and equipment used by hostile forces. This field is very much focused on ascertaining the capability of hostile actors, and while private enterprises have been known to conduct intelligence against competitors' products, systems, and processes, this is generally not included in the category. As with IMINT and SIGINT, it remains a field used exclusively by military- and state-level intelligence organizations.

MASINT (Measurement And Signature INTelligence): The most recent of the major intelligence source categories, MASINT utilizes a range of technologies to determine the characteristics of technical assets. Zachary Lum (1998) in the *Journal of Electronic Defense* describes it as including "radar, laser, optical, infra red, acoustic, nuclear radiation, radio frequency (RF), spectroradiometric and seismic sensing systems, not to mention gas, liquid and solid materials sampling and analysis," but that it focuses "on a target's unintended emissive byproducts, the 'trails'—be they spectral, chemical or RF that an object leaves behind." This highly specialized and technology-intensive field is also limited to military- and state-level intelligence organizations.

OSINT: THE OPEN WORLD

As briefly outlined earlier, the communication and information revolution over recent decades has made available a range of information beyond the dreams of intelligence professionals of previous generations. The most critical element of this revolution has been in cyberspace, with the development of the technology and system architecture of the Internet.

The fundamental feature of the Internet is communication. Where letters still take days or weeks to travel between continents, e-mails are virtually instantaneous. Where fifty years ago intercontinental telephone calls still needed to be made through an operator, Voice Over Internet Protocol (VOIP) technology allows people to connect instantly for almost no cost. In addition, the ability to post information to web pages and make it accessible to any other Internet user has had far-reaching impacts on nearly all fields of human activity.

The field of culture is one area where the Internet has had a profound effect. Cultural issues or trends that may have been isolated to one part of the world in earlier times, or spread over the course of years and decades, now have the potential to become global phenomena within weeks if not days or hours. One example of popular culture that encountered such a rapid spread was the Korean rap song "Gangnam Style" by the artist Psy. This song and its accompanying video became a global sensation within a month of its release, imitated and parodied by people the world over.

Science too has undergone a revolution with the introduction of the Internet. The publication of scientific findings and journals online now

gives an Internet user access to a greater library of scientific data than at any previous time in history. Science has also been revolutionized in its response to crises. One notable example was the role the Internet played in the detection and analysis of the 2003 SARS virus, which caused over 8,000 deaths in 2003. Intelligence gathered by Canada's Global Public Health Intelligence Network provided the first indications of an outbreak of a flu-like disease in China. A global research effort into the origins of the disease was coordinated by the World Health Organization, with information sharing between nations facilitated by online technologies.

Politics too has been transformed. President Obama's election victories in 2008 and 2012 have been widely identified as leveraging the Internet not only to promote his campaign, but to conduct research on key issues and geographic trends, as well as drive fundraising. The Internet allows political messages to be distributed faster and more widely than ever before, while at the same time allowing an unprecedented focus on elected officials' every movement and spoken word.

The Internet and Security: An Intelligence Perspective

Along with the areas outlined earlier, the Internet has had a marked impact on the field of security. While we have briefly examined how it can be used influence domestic politics, we have also had ample evidence recently in North Africa and the Middle East that it can be a facilitator for a range of phenomena from mass discontent and public disorder to coups d'état and civil war. The communication channels of the Internet make it easy for like-minded individuals to band together in groups and create and grow political movements, ideologies, and campaigns of mass action.

The Internet can also provide a forum for political and religious radicalization. While the highest profile incidents tend to involve radical Islamic extremists, it should be considered that similar radicalization can occur in online communities for the far right and for animal-rights extremism.

It is self-evident that the security issues outlined previously have occurred throughout history without the Internet playing any part. However, the critical argument here is that the Internet has a key enabling capacity that can increase the incidence, speed, and scale of security threats. At the same time as increasing security risks, the Internet also provides considerable opportunity and means to observe, deter, and counter such risks. It is in this role that the Internet is of immeasurable value to the corporate intelligence professional.

Security risks in cyberspace can be said to fall into three broad categories. These are *State*-level threats, *Criminal* activity, and cyber *Activism*. State-level threats predominantly involve cyber espionage, or the unauthorized acquisition of privileged data through cyberspace. There have also been a small number of incidents where state-level actors have conducted cyber attacks against physical targets. The most notable example of this was the operation against Iranian nuclear facilities at Natanz in 2010. A type of malware (known as Stuxnet) was designed to specifically target the control systems of uranium centrifuges, manipulating them in such a way as to damage or destroy them.

Criminal activity involves theft through the retail banking sector. In one notable example in late 2012, criminals were able to steal some 36 million Euros from more than 30,000 retail and corporate accounts across Europe. Attackers were able to override dual-factor authentication procedures by having malware infect a user's PC and mobile device simultaneously.

Cyber activism essentially consists of action to initiate or support political or social change. It has been made famous by groups such as Anonymous, and incorporates a variety of techniques, including distributed denial of service (DDoS) attacks, which involve flooding a website or server with a greater amount of data than it can process, making it difficult for legitimate users to gain access. Cyber activists are also known to gain access to privileged online assets for the purposes of exposing private information or embarrassing the asset's owners.

A further element of the Internet worth mentioning here is the "Deep Web." From a technical perspective, the phrase refers to that part of the Internet that is not indexed by standard search engines. While estimates as to the size of the Deep Web vary, Michael Bergman (2001) estimated in a research paper that it was "400 to 550 times larger than the "Surface Web," a factor that is likely to have risen considerably. Much of the information stored on the Deep Web is corporate archives and other data storage, but the Deep Web is also the location for a range of illegal activities ranging from organized crime to hacking and the hosting of child pornography. Much of this information requires specialized knowledge and tools to access, and it is not generally considered to be a useful resource for OSINT information at this time. However, as the cyber security landscape becomes more complex in future, it is increasingly likely to play an enhanced role. Internet relay chat in particular is enjoying increased focus as a result of its role in supporting targeted operations against companies.

Social Media: Networks within a Network

Social media is a key aspect of the information revolution and is a natural extension of the principle of information sharing that underpins the Internet. Social media can be defined as the means by which people interact while creating and sharing information in virtual networks. Sites such as Twitter, Facebook, YouTube, and Reddit are all examples of social media. Where social media differs significantly from the Internet is the scale of its constituent parts. While it is possible for any individual to create a web page and post their own content, this often requires investment in time, money, or technical understanding. Social media, on the other hand, is designed specifically to assist the individual user to create and share information. When an Internet user joins Facebook, the site offers clear instructions on how to post personal information and how to connect with other users. The environment of social media therefore solicits far greater individual involvement than the Internet alone does. In so doing, it creates a far more complex and fluid informational environment.

Like the Internet, this environment presents the corporate intelligence professional with opportunities and challenges. While the vast majority of social media activity will be of no use to OSINT collection, there are likely to be valuable needles in the haystack. Social media's importance falls into two categories

- *Information distribution*: Social media is particularly adept at rapid information distribution. This can range from a corporate marketing team promoting a new product to a news media organization announcing a breaking story. The US Special Forces raid that resulted in the death of Osama bin Laden near the Pakistani city of Abbottabad was actually tweeted in real time by a local resident. Other forms of social media information distribution can originate from threat actors themselves. The hacktivist collective Anonymous runs several active Twitter feeds, while the Izzd al-Din al-Qassam Cyber Fighters, a Middle Eastern group linked with cyber attacks on the US banking sector, is known for advertising its intended targets over social media.
- *Personal activity*: Social media also provides a rich source of information on individuals' activities, intentions, or mindsets. The popularity of social media has led to a significant proportion of the population posting personal information on a regular basis, often seemingly unaware that this information is in the public domain. One example of this was the case of a young woman

in Britain who had started a new job. Finding the position less interesting than she'd hoped, she took to her social media account to share her concerns with her network. Unfortunately, she had added a number of colleagues from her new workplace to her network. They reported her comments to management and she was relieved of her position. While this is perhaps an extreme example, it does highlight that individuals are able and often willing to share more of their personal information and opinions to a wider audience than at any other time in history.

The same concept also applies to groups' activities. Social media not only facilitates individual network connections, but allows groups to connect with each other and with interested individuals. Examples of activist and extremist groups sharing details of intended activity are commonplace on social media. While the groups involved are generally aware that they are broadcasting their intentions, the possibility that they will attract greater support and attention often overrides caution. The same concept holds true for organizers of potentially disruptive public events.

The availability of large volumes of personal information through social media has prompted an extensive debate on the use of this information by the law enforcement and security sectors. It is important to consider the boundaries of privacy in social media, not only with a view to an individual or firm's legal obligations, but also the ethical considerations that should guide the corporate intelligence professional. Social media sites offer a range of privacy options to their users so that they can restrict who can view their information online. Users who do not choose to make use of these may be considered to be placing their information in the public domain; however, the collection and use of this information should still be given due consideration. Information that has only been disclosed to a defined private group can be considered to fall outside the OSINT category.

As a tool for OSINT information research, the Internet and social media are unparalleled in terms of their potential. The speed and efficiency with which specific information can be acquired, whether that be the date and time of a protest march or the principal leaders of the Pakistani Taliban, is virtually instantaneous. More nuanced information collection is more challenging, however, and as anyone who has researched on the web will attest, it is easy to be swamped by the blizzard of information available, or lured off on tangential paths. As with other areas of intelligence, obtaining OSINT information requires planning, skill, and discipline.

Another significant challenge with the Internet and social media is the reliability of sources. The nature of the Internet allows a wide range of individuals to contribute content and information. While much of this information comes from reliable sources and is independently verifiable, there are vast realms of biased, specious, ill-informed, and deliberately misleading content to contend with. Compounding the questionable reliability of Internet sources is the often rapidly changing information environment. An online source may prove consistently useful for a particular field, only to fall into disuse, become unreliable, or be superseded. This element of the Internet drives the need for constant source review, in general far more frequently than more traditional information sources.

News Media: A Similar Perspective

A further critical OSINT information source is the news media. The news media industry in many ways reflects the intelligence environment, with its focus on what consumers need to know, its wide-ranging information collection methods, its analysis of this information through commentary and editorials, and its effective dissemination technologies. Where intelligence differs significantly from media is in its emphasis on offering a decision advantage to its clients.

News media is an extremely valuable source of OSINT information. The range and depth of its information-acquisition capabilities and the generally unbiased reporting of this information is a significant capacity multiplier for the corporate intelligence professional. Reputable news media sources should in almost all cases form a key component of any OSINT collection plan.

Despite its status as a fundamental OSINT resource, there are issues that need to be considered when collecting and analyzing news media sources. Chief among these is a potential for sensationalism. While many reputable news media organizations successfully avoid this, a large sector of the news media is privately owned and is geared more toward a profit-making enterprise. This profit imperative can place tension on dispassionate reporting and analysis by the need to sell newspapers, attract viewers, and drive web page views. Sensationalist headlines or content can be a way to drive this, something that does impact on the quality of information provided.

A further issue to be aware of is the potential for news media outlets to engage in "bandwagoning." This means that the manner in which a news story is reported by one influential news outlet is often matched by other

outlets without sufficient critical analysis of whether the information in the original story is complete and accurate, or whether the conclusions drawn are valid and well reasoned. To some extent, this tendency toward groupthink is driven by the role of the Internet and 24-hour news stations. There is a need to provide news stories as quickly as possible or risk losing market share to a commercial rival. This rapid turnaround and need to match an industry standard can work against editorial independence. While this is by no means a universal trend, the intelligence collection and analysis process must take it into consideration.

Active bias is another concern when collecting information from media sources. This is most notable in media outlets where there is significant state control or influence over the editorial process. Within Western democracies, this tends to be a reduced but still relevant issue. Censorship can of course also impact the quality of news media information. Important events may be stricken from news media sources entirely or may appear in a modified form. In certain countries, there is a tradition of self-censorship among media outlets, without direct involvement from the state.

HUMINT: THE HUMAN ELEMENT

As outlined previously, HUMINT is information derived from direct human contact, or from a traceable chain of direct human contact. HUMINT information can take a number of forms. It can be based on individual relationships, where an intelligence professional is known to the human source. This category could include subject-matter experts such as academics, or others who have made a long-term study of a particular field. It can also include people with extensive experience in a particular field or geographic region who have gained their expertise through long exposure to their environment. It may also include people who have limited experience in a given field or location, but are valuable sources of information due to their being in place and able to observe the environment around them.

Beyond individual relationships, HUMINT can also be founded on liaising with governments through industry groups and through peers. HUMINT sources in this context may not be individuals with whom an intelligence professional has established a relationship, but are nonetheless likely to offer their insights and information out of duty, professional obligation, or courtesy. Many human sources are available to corporate intelligence professionals that may not be immediately

apparent. Initiative and sound interpersonal skills can often leverage surprisingly rich sources of information.

Public sources of HUMINT information can be found through open meetings or conferences. While these sources may not offer the breadth or depth of information as some of the others listed here, they can often offer important insights into issues or highlight useful avenues of further research.

One final category of HUMINT information source is the covert human source. Only in very rare circumstances would a corporate intelligence professional make use of such an asset. Much of the public perception of intelligence is formed by popular culture, involving covert sources and surreptitious meetings in atmospheric locations, but the pragmatic truth is that even in military- and state-level intelligence organizations, the overwhelming majority of information acquired in the collection phase is through OSINT or noncovert HUMINT sources. However, there are times when a covert human source can be highly effective, with one possible instance being complex due-diligence investigations.

As with all categories, HUMINT collection can present significant challenges for the corporate intelligence professional. The first of these is reliability. While stringent efforts should always be made to verify and confirm information from a human source, there are occasions where the source will have access to privileged or unique information that is difficult to verify. In these instances, the historic reliability of the source is useful when assessing the information, but this is not foolproof. Another challenge can be found in relationship management. Often the most effective human sources are the result of a well-cultivated relationship, and maintaining these along with the numerous other pressures on the intelligence professional requires focus and dedication. Subject-matter experts are also likely to be busy individuals with many calls on their time, and the need to respect their professional commitments while also obtaining essential and often critical information must be finely balanced.

COMPANY SOURCES

As a corporate intelligence professional, you will generally find yourself either employed at a specialist intelligence consultancy or on the staff of a firm whose primary business role is outside the field of intelligence and security. In either case, you will be conducting intelligence operations on behalf of a specific company. This company is itself a useful source of information.

This information can be from sources such as subject-matter experts employed at the company, who are able to give insight into the firm's operations, capabilities, and risk exposures. Information may also be available through frontline sources such as security guards reporting increased threat activity, indigenous staff employed by the company in their native country giving insight into their local communities, and even customer service and human resources staff reporting on customer and employee concerns.

Company sources can also extend to project plans, meeting minutes, and the company's internal website. Internal company records can also provide a significant source of information into previous security challenges faced by the company, the manner in which they attempted to address those, and their degree of success. In the same manner, internal sources can also give insight into the challenges faced by the company's industry and the marketplaces in which they operate.

These sources may, in the normal run of business, be categorized as HUMINT and OSINT; however, they serve a different function in the intelligence cycle in that they give the context in which external intelligence may be assessed. The critical question that must be answered when analyzing information is "Why is this important?" Utilizing company sources is a critical stage in developing an answer to that question. The corporate intelligence professional who disregards this aspect will likely find their efficiency significantly restricted.

THE COLLECTION MANAGEMENT PROCESS

In our discussion of OSINT, HUMINT, and company information sources, we have gained something of an insight into the potential complexity of the collection process. In order to operate an efficient and effective intelligence capability, it is critical that the collection management process be effectively planned and executed.

Planning

The planning stage is central to an effective process. This is generally the responsibility of an intelligence manager and is in response to previously defined intelligence requirements. Stages of an effective planning process may run as follows:

- *Internal resource evaluation*: Prior to establishing a collection plan, it is critical to understand what resources are available for its execution. This includes determining which qualified staff are available for the task and how many work hours per week they can devote to the task. What is the forthcoming work schedule for the intelligence team? Is it likely that the same resources will still be available over the coming period? Are the necessary IT and communications assets available? Is it more efficient to outsource the collection for a particular project or to keep it in-house?
- *Source evaluation*: The next stage is to determine which sources are available across the OSINT, HUMINT, company, and possibly other collection categories. How efficient are these sources? The collection team may have access to multiple blogs and news sources published on an area of interest, or their only source may be a local mine manager who is difficult to reach during normal operating hours.

These two stages will give insight into the burden that effective collection will place on the intelligence team. If the intelligence manager determines that they have insufficient resources, it is critical that this be communicated to the client, along with an estimation of which intelligence requirements could be addressed at current resource levels.

Once the resource and source evaluation stages are complete, it is essential that the findings be recorded. Often, the simplest way is to populate a spreadsheet with the following information:

- The list of intelligence requirements
- The human and technical resources available to conduct collection
- A detailed source list to be monitored on a regular basis
- A list of broader online search terms that will complement the formalized source list

An important final step is to schedule a formal a review of the collection plan at regular intervals to respond to any changes in intelligence requirements, resources, and available sources.

Execution

There are three potential models for information collection. The first of these is based on a *finite research* task. In this model, the researcher is given a specific research task to undertake within a limited time period,

and the process is target-centric. An example may be a request to research recent attacks attributed to animal rights extremist groups in the Pacific Northwest of the United States, and the time frame may be two days. Information obtained under this model would allow an analyst to create a snapshot assessment of the threat.

A second model is to conduct *periodic research* on the same topic. In this instance, a researcher may be tasked to monitor the same animal rights extremists groups on an ongoing basis. This would involve a daily or perhaps weekly checking of sources for relevant information. This model allows a more nuanced analysis, one that is able to track long-term trends and draw greater insight into the groups' activities and cycles of operation.

A third model would be to assign a researcher to conduct an *exploratory* research project. An example of such a task might be to search for any potential threats from activist groups in the Pacific Northwest to hunting and sportswear retailers. This approach is especially useful in determining the security environment within a specific industry or region, which can allow more extensive intelligence requirements to be developed.

Source Gathering Techniques: OSINT

As discussed earlier, the vast majority of OSINT information collection can be conducted online. In the simplest sense, this may involve entering a term into a search engine and collating the results. However, as an intelligence project's source list expands, researchers will find themselves visiting an increasing number of websites and social media pages to obtain relevant information. As anyone who has conducted large-scale Internet research projects can attest, this procedure is often wearying and inefficient. While an online source may require daily checking under the collection plan, there is no guarantee that each daily visit will bring new and useful information. Each time the target source is checked, however, it makes demands on the researcher's limited time, energy, and patience.

Fortunately there are a number of technical solutions that can assist the efficiency of online research.

- Most major websites providing regularly updated content will offer a number of ways in which a user can track these updates without having to visit the site repeatedly. *Data feeds* operate on the principle of pushing information to the user rather than the user having to pull the information from the site. Data feeds come in a number of formats, with the most popular being the

rich site summary format, or RSS. RSS feeds are indicated on most websites by a distinctive orange icon. Other common data feed formats include ATOM and, less commonly, {JSON}.

RSS feeds can be imported into a stand-alone program known as an RSS reader, specifically designed to render a multitude of feeds in an organized and convenient fashion. The majority of these programs are free to use. Each time the relevant website posts new content, the data feed will also be updated. The RSS reader will constantly and automatically check for such updates and will post the new content in a similar manner to popular e-mail clients. The benefits of using this system are that it allows a single user to read a wide range of information sources without having to type each website's URL in their browser and wait for it to load. It also eliminates wasted visits to sites that haven't posted new content since they were last checked.

- Many websites also offer an e-mail subscription service to users in order to push new content out. Subscribing to these is another convenient way of collecting information that would otherwise involve laborious website visits. This is a highly effective way of receiving specialist reports and publications from think tanks, industry groups, and security companies.
- A further technique to assist with gathering OSINT information is to utilize a database of previously collected sources. This offers invaluable assistance when tracking trends or providing background to a new threat issue or area. Critical information may have previously been gathered by your company, which, if properly stored and indexed, can save a researcher a significant amount of time and effort. The importance of storing information is discussed later in this chapter.

Source Gathering Techniques: HUMINT

Techniques for gathering information from human sources vary significantly, dependent on the nature and status of the source. At one end of the spectrum may be a trusted and well-known colleague who is simply a phone call away; at the other extreme may be a covert source who must be handled with great psychological care and consideration for their own security. While human sources can be capable of providing high-value information not available through other sources, an important caveat with human sources is an enduring perception of them as a silver bullet or having innate

virtue over OSINT or other information sources. Therefore it is critical to assess the utility of human sources for a particular intelligence project, and this is often a decision that rests with the project's intelligence manager.

When engaging with a human source, it is important that the ethical and legal environments be assessed and that the intelligence manager be satisfied that the firm's obligations in these areas will be discharged while obtaining information from the source. While the misrepresentation of an intelligence researcher's identity may be a viable strategy for military- and state-level intelligence organizations, private individuals and companies are held to significantly different ethical and legal standards. It is therefore advisable that human sources be aware at all times that they are speaking to an intelligence researcher in their professional capacity and that information supplied will be used for commercial purposes. In certain cases, information may be provided under certain restrictions (such as under the Chatham House Rule*). In these cases, it is important to abide by such conventions. Maintaining ethical conduct is important to maintain not only the reputation of an intelligence professional and the company, but for the industry as a whole. Honest, professional, and ethical conduct is also likely to strengthen relationships with human sources.

A key element of HUMINT information gathering is planning. Human sources are oftentimes poor, and their availability can be limited. Therefore it is critical that the intelligence researcher obtain the maximum benefit from the limited time and opportunities available. Key to this is planning which questions to pose to the source and predetermining as far as possible which follow-up questions would be most valuable to the source's possible answers. A human source may wish to engage with the researcher but may not wish to provide all information requested. Therefore a process of elicitation should be detailed, logical, and persistent.

Once information has been obtained from a human source, the researcher should attempt to verify it through other sources, or if the information is unique, its plausibility should be examined in the context of other sources of information and historical records.

* "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." This rule originated at the Royal Institute of International Affairs (Chatham House) with the aim of giving anonymity to speakers and to encourage information sharing. It is now used more widely as an aid to free discussion, and so this is regularly quoted at security meetings worldwide. Without this courtesy, it would be much harder for corporate intelligence analysts to do their job!

Source Gathering Techniques: Company

Gathering information from within your own company may be expected to be among the easiest forms of intelligence collection. While modern companies do make a significant amount of information available internally, this area can still present a significant challenge. In part this is because the function of security intelligence can often be poorly understood within firms not operating directly in that field. This has the potential to create a degree of mistrust toward the security intelligence function.

Business leaders may also be concerned that intelligence represents a cost rather than a profit-making area of their business, further complicating efforts on the part of the intelligence professional to gain a comprehensive understanding of the company's operations, policies, and procedures. Any such reluctance is often best countered by engaging with people across the business and demonstrating how security intelligence can provide a decision advantage to the firm in general, but also to their business unit in particular. In this context, it is no longer sufficient for an intelligence professional to solely rely on skills in security and intelligence; instead, the intelligence professional must be able to demonstrate a commercial awareness and readiness to engage with other business units. A foundation of trust and strong personal networks is arguably the most important asset in this field of collection.

Information Archiving

Earlier in this chapter we touched on the importance of being able to access an archive of previously collected information. Such a resource is invaluable in maintaining efficiency during staff transition, but it is also useful in detecting trends and providing context to new and emerging threats. Recording each item of information at the collection stage can also be critical if an item of analysis is questioned by a client or if the source of a particular item is requested.

One of the simplest forms of recording collected information is through a spreadsheet. This format is advantageous in that it provides a simple tool, not requiring significant IT knowledge, that is still capable of organizing and manipulating large volumes of information. (See Figure 7.1 for an example of a source database spreadsheet.)

Another simple form of recording collected information is through the RSS technology discussed previously. The majority of RSS readers are capable of storing large volumes of posts as well as providing search and

Source Register Template

Source Register													
Serial	**Source Identifier**	**Name**	**Home/Host Community**	**Organization**	**Principal Handler**	**Co-Handler**	**Preferred Method of Contact**	**Telephone Number**	**GSM Number**	**E-Mail**	**Access**	**Date of Last Contact**	**Date of Next Contact**
001	K19	CLAUS, Santa	GROTTO	HARRODS	M23	J17	Letter stuffed up chimney	+44 (0)209 059 9988	+911 (0)7111 123456	StNiklaas@NorthPole.org	the best - can tell us everything	2010-12-25	2011-12-25
002	D01	MOUSE Mickey	CASTLE	DISNEY WORLD	T21	G76	via Sky TV	none	none	bigmick@disney.com	Has the lowdown on that evil duck	2011-03-28	2011-03-31
003	R11	BIGFOOT	YUKON	SAVE THE FORESTS	M23	T21	We don't contact him – he contacts us			hairystinker@STF.org	believed to know where the next big gold strike will occur	2009-07-21	not known

Figure 7.1 Source register template. (Courtesy of Steve Phelps, S&I Solutions Ltd.)

filtering functions to locate particular items of interest. Maintaining these systems and regularly backing up their database components is a relatively easy task with significant potential value.

The storage and collation of research information is the subject of the following chapter, which will engage this issue in much greater detail.

Verification

The verification of data sources is an important if limited element of the collection process. As researchers examine various items of information, they are well advised to adopt a critical mindset during the process. A rapid assessment of an item or source of information can be driven by a relatively simple set of questions. Some examples are as follows:

- Is this item relevant to the intelligence requirements?
- If we have used it before, have we found it to be reliable? Is it possibly misleading, the work of propaganda or a provocateur?
- If we haven't used it before, can we assess it to be credible? Can we believe the information it contains?
- Is the source likely to be accurate? Is there a potential that it has been embellished or had important information redacted?

This process should be a constant companion to corporate intelligence professionals engaged with collection. Not only do they face the responsibility of locating and obtaining relevant information, but they are also responsible for the initial stage of quality control. A phrase coined early in the development of mainframe computers has relevance here; computer engineers would warn end users that "garbage in would mean garbage out," i.e., flawed information processed through a computer would result in a flawed output. The same holds true for the analysis stage of the intelligence cycle; flawed sources will lead to flawed analysis, regardless of the skill and dedication of the analysts at work.

The Review Process

As we have seen earlier in this book, an entire stage of the intelligence cycle is devoted to reviewing the intelligence product as a whole. This formal process is invaluable, but it should not prevent collection researchers from reviewing their sources and their approach at other times, and if necessary escalating concerns or shortcomings to the intelligence manager.

CONCLUSION: BETTER EQUIPPED THAN EVER?

The collection stage of the intelligence cycle can represent a daunting challenge. The sheer scale of information available to the modern intelligence researcher, problems with source assessment, and keeping up with a highly dynamic information environment can be a considerable burden.

As we have seen, OSINT dominates the field of corporate security intelligence, and the Internet and social media dominate the field of OSINT. This information environment is complex and dynamic, and this is only expected to become more so as increasing numbers of users and devices are connected and as technology continues to evolve. This places an obligation on collection researchers to be dynamic in response and to constantly review the utility of the information they are collecting.

HUMINT and company sources also offer a range of challenges, but these can be rewarding if the researcher is able to invest time and effort into their development.

While intelligence researchers undoubtedly face a significant challenge, they are also better equipped than at any time in history to face it. We have only touched lightly on the range of tools and technologies that can assist in the collection process; indeed, the very systems that complicate the process can often be harnessed to meet that challenge.

8

Collation

CHAPTER OBJECTIVES

1. To emphasize why collation is such an important activity, despite often being overlooked.
2. To discuss some of the common failures of collation, which can undermine the intelligence process.
3. To introduce the key concepts and best practices around collation activities in the corporate environment.

INTRODUCTION

The collation element of the intelligence cycle is often maligned and neglected in studies of the subject, but it is of vital importance. Though an efficient and accurate process of collation is no guarantor of good analysis, an unsuitable, underdeveloped, or even absent collation system can effectively hamper the workings of analysts and prevent the production of quality actionable intelligence. If an appropriate level of attention is diverted to establishing and maintaining a dynamic process of collation, then a considerable burden can be lifted from the shoulders of analysts, echoing the age-old aphorism that "a stitch in time saves nine."

As noted in the previous chapter, the term *collation* first appears to have gained traction in intelligence circles around the time of the First World War, although it was not systematically assessed as part of the

intelligence cycle until several decades later. This is partly due to the lack of formal consideration of intelligence processes until after WWII. However, it can also be attributed to the lack of requirements for codified procedures of collation due to the relatively small volumes of intelligence that required processing.

Accordingly, a combination of more expansive intelligence requirements and greater avenues for collection require the development of a more rigorous collation process. Both of these factors are significant in the context of the corporate security intelligence environment. Firstly, the ability to expand intelligence requirements beyond the narrow and negative conception of security intelligence to one of a source of opportunity for a corporate entity significantly enhances collection requirements and opens up new areas as potential subjects of intelligence gathering and sources of revenue for the business. Secondly, the astronomical increase in terms of the volume of information available, both in terms of the variety of forms of intelligence (HUMINT, SIGINT, SOCMINT, etc.) and the ever-expanding volume of data within those subgroups, means that the process of collation mandates proper attention by the intelligence function.

KEY PRINCIPLES

Regardless of the complexity or nature of the information set out in the intelligence requirements or collection plan, a fundamental principle of collation is the *standardization and harmonization of incoming data*. Thorough adherence to a coherent and consistent process of data input may appear overbearing at this stage, but such an approach provides a platform for analysts to link inputs and identify emerging patterns, which can prove crucial in assisting the production of accurate analysis or provide important insights in their own right. Again, the challenges associated with standardization vary significantly according to the nature of the input and the form of intelligence that is provided.

Starting at the simpler end of the scale, a "structured" data input tends to exist in a preformatted form, by its nature. Examples of structured data include telephone numbers, names, and e-mail addresses. The conventions surrounding examples of such data inputs ensure a certain degree of standardization. For example, current conventions surrounding e-mail addresses dictate that all feature the @ sign that separates the local and domain elements of the address, which would necessitate their input into a database in this fashion.

WHAT'S IN A NAME?

Failure to input supposedly simple data such as the target of an intelligence-gathering operation can have significant ramifications, as two recent cases have demonstrated. The Nigerian Umar Farouk Abdulmutallab, colloquially known as the "underwear bomber," was arrested after his attempt to bring down a Northwest Airlines flight from Amsterdam to Detroit on 25 December 2009. Abdulmutallab forged links with Islamic extremists during his time as a student in the UK, and his subsequent contact with leading al-Qaeda propagandist Anwar al-Awlaki had already been documented by various elements of UK and US intelligence in the months leading up to the attack. In November 2009, his father visited the US Embassy in Abuja to detail his fears about his son's radicalization and alert them to the possibility that he was involved in an impending attack. However, a spelling error when Abdulmutallab's name was initially input into the Terrorist Identities Datamart Environment (TIDE) database delayed recognition of this latest development. Subsequently, US intelligence services overrode the decision to revoke Abdulmutallab's visa (designed to be the tripwire for any potential operation), allowing him to board the flight with near-undetectable explosives stitched into his clothes.

Similarly, the elder Boston Marathon bomber, Tamerlan Tsarnaev, was initially able to elude detection on his 2011 flight to Russia, where his personal process of radicalization allegedly took place, because of an Aeroflot employee's misspelling of his name in the flight manifest. It was not until Russian authorities coordinated with their American counterparts that they became aware of Tsarnaev's trip abroad.

Even within this comparatively simplistic subset of structured inputs, forms such as names can pose problems because of their susceptibility to interpretation and alteration. This can be illustrated by the Chinese tendency to present the clan or family name before the given name (e.g., Xi Jinping's father was named Xi Zhongxun), which can cause confusion and failures of collation if not accounted for in the process. Similar discrepancies can occur over dates, addresses, and other ostensibly basic forms of input.

Furthermore, accuracy and attention to detail are also crucial at this stage, as the most basic of errors can lead to issues further on in the processing stage of the intelligence cycle. In the context of names with

multiple variations on spelling (e.g., Muhammad could also be spelled Mohamed, Mohamad, Mohammed, Muhamet), it is often the best policy to defer to the most common version for reasons of simplicity, even if it may not be the most accurate or technically correct. Wikipedia is sometimes a useful guide in this sense, since it provides an already standardized basis of spelling, although it is still not infallible.

Depending on the likely frequency of such instances, the collation process can benefit from the introduction of an approximate string-matching feature, also known as *fuzzy string matching* or *fuzzy spelling*. The use of these features can obviate situations where a previous input that could be vital to a piece of analysis is missed because of a formatting or spelling error in the input or retrieval process.

STRUCTURED VERSUS UNSTRUCTURED DATA

The difficulties that arise with this process of input of structured data are multiplied when considering its unstructured counterpart. Unstructured data consists of those forms without preformatted models, including text, images, audio, and video, which tend to form the bulk of the material collected for intelligence analysis. Put simply, the means by which humans understand and process information and the way in which computers do it are vastly different. Whereas cognitive studies have indicated that humans understand by linking networks of the concepts that are contained within sentences, rather than the full sentences themselves, which contrasts entirely with the machine's means of computing information.

The challenge for those responsible for collation is to develop a suitable method for bridging this gap by standardizing and logging this incoming information so that the data is presented in a clear and digestible manner for the subsequent process of analysis. Alternatively, if this function is not performed to a satisfactory standard, analysts are presented with the additional task of performing the collation process on top of their analytical role, which is likely to have a detrimental impact on the timeliness, accuracy, and relevance of the intelligence ultimately produced.

Again, the specific tools and techniques suitable for this process of harmonization and standardization of incoming data can vary significantly according to the complexity and scope of the intelligence requirements. In some cases, where inputs come in the form of manipulable text, the process of collation can be as simple as logging their date,

origin, subject, and other details and then transferring those inputs into a searchable central or shared location for later retrieval by an analyst. This may particularly be the case where the bulk of unstructured data inputs are sourced in an intermittent fashion from open sources, such as online reporting from newspapers. Nonmanipulable text (e.g., in the form of handwritten submissions, or possibly even recorded statements) may need to be transcribed into a consistent format for an analyst's perusal. Alternatively, if a brief synopsis rather than the content of the report or incident is required, rudimentary databases in the form of spreadsheets, created using Excel or similar products, can be used.

DATABASES AND AUTOMATED COLLATION

Using Excel offers the simplicity of a comparatively straightforward and user-friendly interface (which is already common in the corporate environment). However, when the process of collation is required to draw links between one piece of data and many others, rather than a one-to-one basis, then a dedicated database program is likely to be more suitable. Object-relational databases are useful in this regard. These can essentially map connections between many different tables, and so can be useful for spotting connections in large amounts of data, e.g., phone records or address lists. In these databases, the input tables will often already have been collated, and so the database effectively helps the analyst/interpreter pull all relevant material through the use of structured queries. Such a database may also pull in external feeds, allowing for real-time matching of relationships. This is very powerful, particularly in investigative work, but can be more complex to pull together and host. Visualizations can also be complex, although emerging software is helping to change this.

Stepping up a rung on the ladder of complexity, a regular and systematic collection effort that deals with a greater volume of inputs may mandate the development of an automated process of harmonization. Continuing with the previous example of open-source online newspaper reporting, RSS (Rich Site Summary/Really Simple Syndication) feeds can be harnessed to pool all potentially relevant inputs into a single interface in the form of an RSS reader.

Such tools can automatically provide crucial metadata in a common format to contextualize the actual content of the inputs, such as authorship, date, and time. In this context, metadata essentially means

WHAT TO DO WITH METADATA? SOCIAL NETWORK ANALYTICS AND HYPERMAPPING

Social network analysis refers to the application of network theory to the study of social networks, often representing in a visual format. Largely because of the accessible format in which the information is presented, this practice has recently increasingly been focused on online social networks, such as Facebook. Relationships between actors are identified and explored to understand how individual actors and groups that may be considered as threats interact with each other. Regardless of whether an intelligence operation is able to consider the content of messages sent between actors, or "nodes" in the language of network theory, a study of their recipients and the frequency of communication can offer insight into organizational structure and the source of the key actors and linkages within the group. Network scientist Valdis Krebis's analysis of the communication linkages between 9/11 organizers and perpetrators was particularly informative, owing to its ability to clearly identify the centrality of ringleader Mohamed Atta to the development of the plot.

An alternative application of metadata to enhance the collation process is the use of hypermapping. A hypermap is defined as a georeferenced multimedia system that can structure individual multimedia components with respect to each other and to the map, which can allow a collator to navigate data both thematically and geographically. Though a significant volume of data is required to establish a functional system that adds value to the collation process and contributes to greater understanding for analysts, such techniques can be illuminating and offer unique insights when employed successfully. Former NSA subcontractor turned whistleblower Edward Snowden's revelations included details of such a program called Boundless Informant, a program that reportedly sought to identify patterns in channels of communication within states such as Pakistan and Iran imposed onto a map in real time. Corporate analysts can only dream, but these capabilities are becoming more and more the norm.

"data about data," and systematic consideration of this field can in itself provide unique analytical insights. The value of such an approach can be enhanced considerably when applied to other avenues for intelligence gathering, such as social media, which—despite the best efforts of the supplying companies—can still be mined comparatively cheaply and easily in order to gain insights.

For example, the ability to gather information regarding the time, authorship, location, and content of any hostile tweets, or other posts made on social media platforms, can be extremely useful for the corporate security intelligence manager. When a large volume of such incoming data can be collected, techniques of this nature provide the ability to store and cross-reference such material in object-relational databases that can allow an analyst to study any patterns and trends that may be emerging. When data is packaged in such a fashion, an effective process of collation can add value to intelligence, rather than operating merely as a stage of drudgery.

BIG DATA

The pinnacle of complexity in terms of collation is reached with the ascent to *big data*, a currently trendy term that refers to datasets so large that conventional means cannot be used to collate and process the incoming information, mandating the use of highly customized and sophisticated tools. As alluded to earlier, the move toward big data has been prompted by technological advancements and the propagation of a variety of collection techniques.

There is considerable interest in the insights offered by big data, particularly in the marketing world. In the security department, the utility is generally slightly less obvious; indeed, there are numerous challenges. Harnessing this amount of data will be a problem for most security departments, but if collection is likely to be difficult, analysis is even more so. In many cases, the vast extent of the resources required to successfully collate, process, and then analyze such a volume of data means that acquiring it may be an exercise in futility. Instead, leveraging the data being collected elsewhere in the organization—or by external parties—is perhaps the best way to deal with this angle. Ultimately, as ever, it is important to remember that this is not a silver bullet and that people and process have to work in harmony with the technology to bring about results.

GIS

A final part of collation is geospatial intelligence analysis, or GIS. Put simply, this involves plotting things geographically and occasionally also over time. This is very powerful, as a picture can tell a thousand words—especially to the busy corporate reader. For example, a map showing where events have occurred over the last three months in a given country may very much help illustrate the safety levels in various areas. Other data can also be fed onto the map, e.g., locations of travelers, or company sites, along with their size and criticality (Figures 8.1 and 8.2).

ArcGIS remains one of the most popular corporate tools, although there are free alternatives that will reward the user happy to invest the time and effort. A great feature of GIS programs is that they tend to refer back dynamically to a file or database, so they can readily be updated to reflect the latest situation. They therefore combine several elements of collation, and they can even be used as rudimentary databases in their own right (i.e., by using the GIS program to manipulate and edit the data).

Ultimately, all GIS needs is the latitude/longitude of events, posts, or any other data that can be mapped. It is often easiest to capture this at the source. Where this cannot be automated, the process of "cleansing" data offers an opportunity for an operator to go in and add this data. Many tools, including Google Maps, allow the user to select the coordinates of a point; so for example, a news report of a bomb at a certain location can be turned into a usefully plotted piece of event data. Speaking of Google Maps, the explosion in open-source web-based platforms that allow for engagement really are making it easier than ever to collate data geographically. On a side note, Scribble Maps is another service that allows for easy labeling of features; this is not quite collation, strictly speaking, but a very useful aid to visual presentation and analysis.

CONCLUSION: GETTING THE DUCKS IN A ROW

Given the increasing volumes of data available, collation is becoming ever more important to help analysts spot connections and "join the dots"—the essence of the intelligence process. The better the quality of the data, the better is the output. This ties in with the whole concept of knowledge management, as discussed previously, and many of the points raised there are of relevance here (especially in regard to

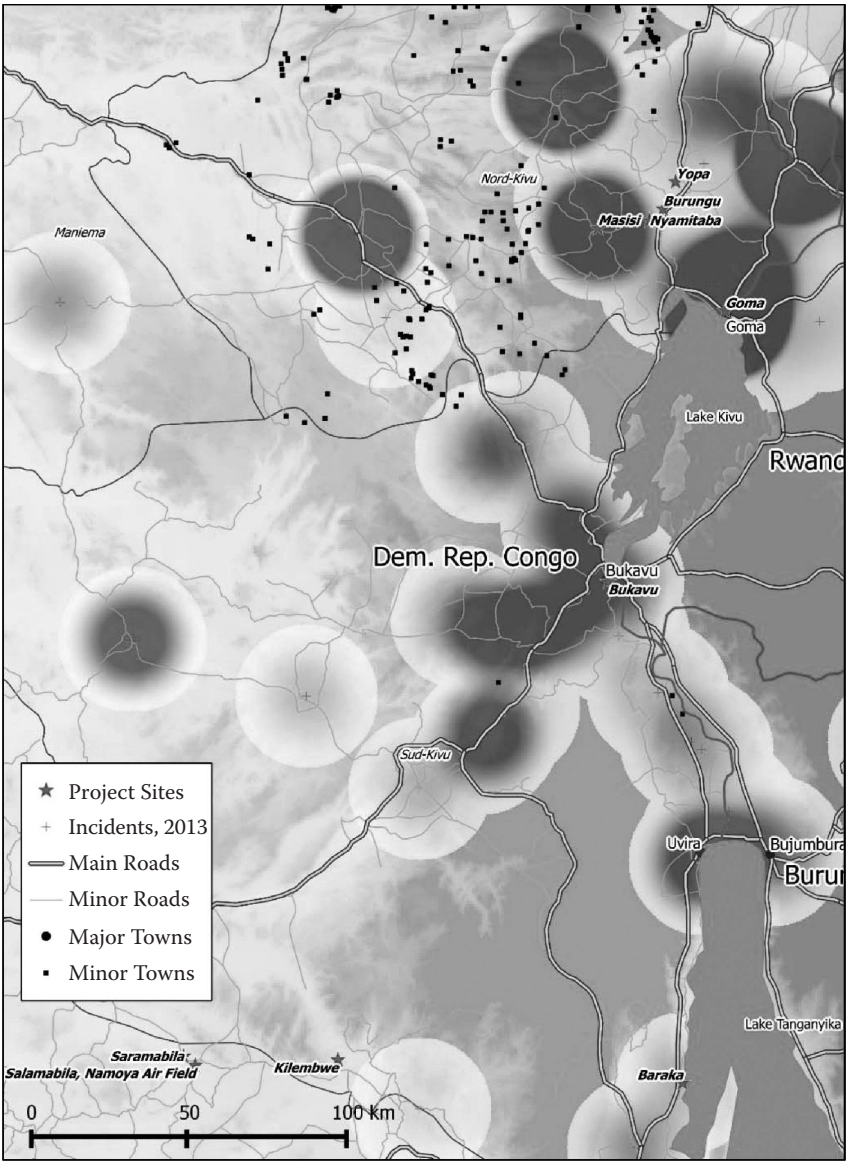

Figure 8.1 GIS in action: Heat map of incidents in the Eastern Democratic Republic of Congo versus NGO sites, 2013.

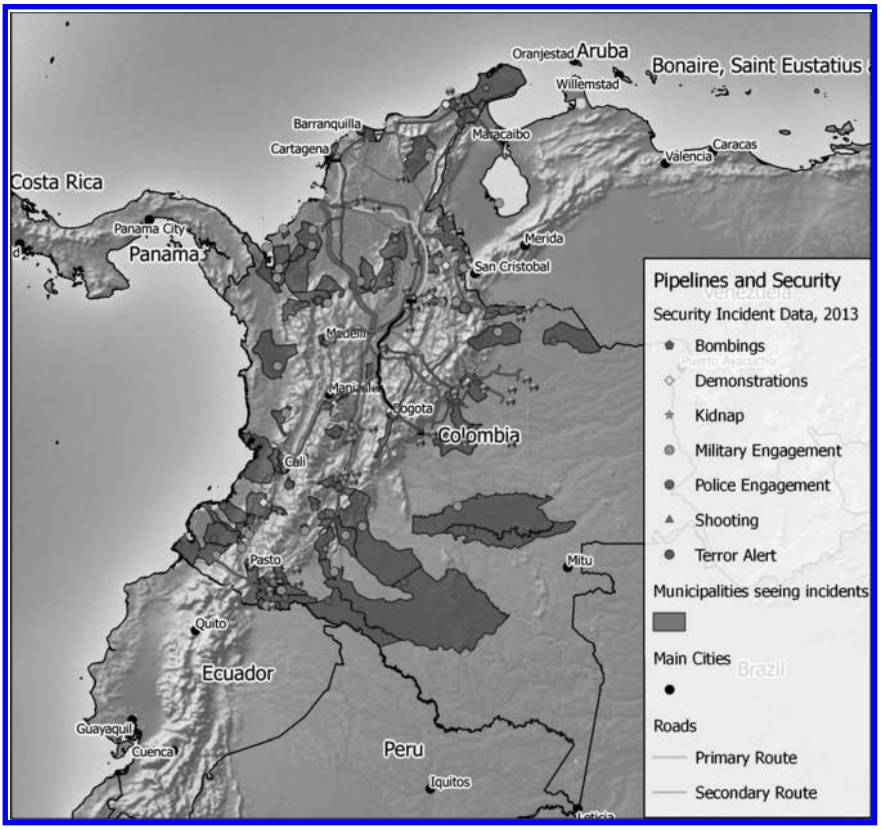

Figure 8.2 GIS in action: Colombia pipelines mapped against incidents, 2013.

standardization of data). Ultimately, it is surprising how often the clues were in fact available to the intelligence team, but they were missed due to someone not making the connection. This is inevitable, given the uncertainty we have to deal with, but the more we can do to control this, the better.

9

Analysis

CHAPTER OBJECTIVES

1. To identify three major models for corporate intelligence processing.
2. To understand how intelligence analysis should begin, and its objectives.
3. To examine how sources should be evaluated to ensure that information is credible before analysis can begin.
4. To understand the central role of the analyst.
5. To outline the differences between intelligence in the corporate and government worlds.
6. To learn a selection of analytical techniques and thought processes.
7. To understand how and why analysis sometimes breaks down.
8. To learn a number of techniques to avoid major analytical pitfalls.
9. To highlight the importance of effective conclusions and summaries.

INTRODUCTION

As previously discussed, the collation and analysis phases of the intelligence cycle are collectively known as *intelligence processing*. This reflects the way in which raw, accumulated information is grouped together in meaningful ways (collation), and then analyzed in order to explain uncertainties and to build "knowledge" (analysis). Most of the literature on intelligence analysis (IA) focuses on state activity, i.e., analysis in

government security agencies, law enforcement, and the military. The main differences between state and corporate IA are that state agencies tend to deal with far greater amounts of "secret" intelligence (protected information that state, criminal, or terrorist adversaries want to keep secret), occasionally supplemented with open-source intelligence. In contrast, corporate analysts focus predominantly on open-source intelligence, supplemented with contextual information from trusted contacts. Sir David Omand (2010) has made a useful distinction between secrets and mysteries. While states have a greater interest in discovering secrets (knowable but secret facts or information such as enemy order of battle), both state and corporate intelligence entities must analyze mysteries (nonconcrete, unknowable information, such as the intentions of state leaders or the implications of multifaceted scenarios). In the corporate sector, the specific way in which intelligence processing is carried out is dependent on the structure, objectives, and customers of intelligence. These factors are shaped by the industry in question, the threats it faces, and the budget allocated to a security department. Intelligence processing may be conducted in-house or by an external provider.

THREE MODELS OF CORPORATE INTELLIGENCE PROCESSING

The different models of corporate intelligence processing can be roughly divided into three categories:

1. Intelligence assessment
2. Target-centric investigations
3. Criminal pattern analysis

An intelligence team may conduct analysis in one or more of these areas, and the boundaries may be blurred. However, this is still a useful framework to aid understanding.

Intelligence assessment is by far the most common form of intelligence function in the corporate sector. It involves the synthesis and analysis of open-source and sensitive information on tactical, operational, or strategic issues, and the production of concise, actionable reports. In the tactical realm, in the oil and gas sector for example, intelligence analysts might produce reports on sightings of militant or criminal activity near company facilities.

These may prompt an immediate response from security teams or a call to law enforcement. At the operational level, analysts may produce intelligence for local security managers tasked with implementing company strategic-security-strategy at the tactical level. For example, an analyst in the pharmaceutical sector might report on the activities of a number of hostile single-issue groups in a region who have shown intent to target the industry, an issue of stated concern by a chief security officer. At the strategic level, analysts might report on political, economic, and security trends that may influence the strategic and operational decision making of either a chief security officer or a company board when an issue is particularly serious. For example, an analyst may report that an upcoming election or expected downturn in an economy will likely prompt violent outbursts in a country in which a company has significant interests.

Target-centric investigations are those that involve tracking and analyzing the actions of an individual or group that poses a threat to a company or industry. Processing in this category will often involve the collation of open-source personal information data and analysis of an adversary network. As an example, an analyst might map the network of a group that is hostile to a company's actions and has targeted the company with malign reputational or criminal attack. Such analysis will often be shared with law enforcement agencies that often have limited time to conduct such thorough, preemptive investigations.

Criminal pattern analysis is perhaps the least common intelligence function for the corporate sector, since in the main it is carried out by law enforcement. In particular industries, however, it is of vital importance. It tends to be applicable to those larger industries that are targeted frequently by multiple criminal gangs in multiple areas or jurisdictions. Criminal pattern analysis is the practice of recording crime data and then analyzing it statistically in order to elucidate patterns of activity. For example, a telecommunications company might analyze incidents of cable theft temporally and spatially in order to assess what their main vulnerabilities are and decide how to take preventive action. Again, such analysis may be shared with law enforcement, and the security team has a vital role in effectively interpreting between the business and the police/security services (see Section 1).

DECOMPOSING THE TASK

Before intelligence processing can begin, it is essential to think about the intelligence priorities that are driving activity. Priorities can be directed by senior staff in the form of Requests for Information (RFIs) or Intelligence Requirements (IRs). Alternatively, analysts may often set their own priorities, since they are trusted as experts in their field and so are tasked to highlight things that are of relevance to management. Regardless of the origination, priorities/IRs must be decomposed into component parts before analysis can begin (Figure 9.1).

A number of crucial questions should be asked:

- Who has prompted the request?
- What is the crucial intelligence question?
- Why is the issue important?
- Has the question been answered before?
- Who are the main customers for the analytical output?
- Which other stakeholders have an interest in the outcome, and how should this be considered in the analysis?
- What are my first impressions of the task and its likely answers?

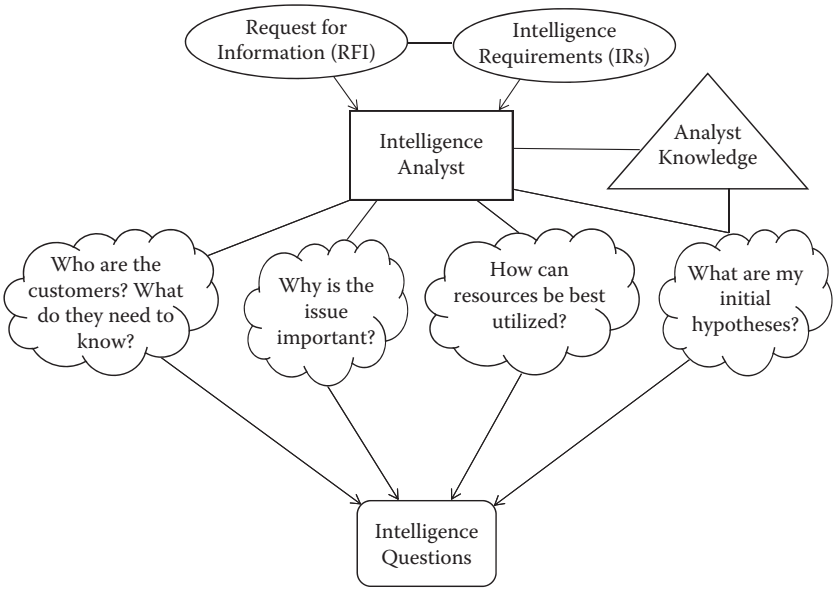

Figure 9.1 Task deconstruction.

- What sources are available to answer the question?
- Does anyone else in my team have relevant knowledge or experience concerning the task?

The decomposition stage addresses the issues of who the customers are and what they will likely need to know; how resources can be effectively brought to bear, avoiding duplication; and the identification of initial, instinctive hypotheses. A key component for efficient analysis is the conversion of "issues" into "questions" that can be specifically answered (Davis 1997). In target-centric investigations, question formulation will usually be quite simple, e.g., "How does subject X connect with members of group Z?" In intelligence assessments, there are normally multiple overlapping and implicitly held questions, such as "What economic or political developments will lead to instability in country A?" Or "Which security developments are most relevant in assessing the threat to foreigners in country B?" It is always helpful to explicitly state and record these to keep the analysis on track when working through information and data.

ASSESSING SOURCES

In the government sector, the collection of information will more often than not be carried out by HUMINT (human intelligence) or SIGINT (signals intelligence) operators, separate to the analyst. In the corporate sector, an analyst may have a researcher/collator, but in the majority of cases, he or she will conduct the majority of research as part of the total task. In both cases, it is the role of the analyst to assess the reliability of sources. Again, a number of questions must be asked.

For all sources:

- Has the source proven to be reliable in the past?
- What are the source's underlying biases?
- Is the source reporting a first-, second-, or third-hand account?
- Is there a possibility of deception?

Specifically for human sources:

- Does the source really have the access that he/she claims to have?
- Does the source have the expertise needed to adequately assess the complex issue in question?
- Is the source simply saying what you want to hear?
- Is the source under any duress?

Source reliability can be checked via two main methods. The first is to assess whether the information provided is consistent with an analyst's best judgments and knowledge. The second is to cross-check the information with other sources that are known to be reliable. If the analyst conducts his own research, then assessment can take place concurrently with collection. If a separate collector is utilized, then sources must be assessed before analysis can take place. In OSINT (open-source intelligence), the form of research most corporate analysts will be engaged in, assessment is usually carried out on online sources such as news stories, blogs, and social media. No source is neutral. Even the British Broadcasting Company (BBC), which aims to promote a nonpoliticized account of international events, is biased in the sense that certain stories are selected or dropped, and the focus reflects a Western interpretation of the world. For example, watching Russia Today and the BBC alongside each other during the Ukraine crisis of 2013–14 shows how similar facts and information can both deliberately and accidentally be "spun" to suit narratives and perceptions, regardless of official interference. Some online sources have a more obvious or even acknowledged political stance (pro-regime news channels, for example). Others may exhibit more subtle bias: Some global channels may appear to be promoting a neutral standpoint but are actually funded by organizations that are seeking to exert influence on issues that concern them. Often, identifying this bias requires careful long-term work and assessment—emphasizing how source validation is a constant effort in its own right, and a vital process.

COLLATION

Collation was discussed at length in Chapter 8. Again, the process is influenced by the objectives of the intelligence task. Information for "intelligence assessments" will likely be text-based and may be best categorized and stored within word-processing-style documents. Incident information can be stored in spreadsheets or relational databases. Target-centric analysis (including most due-diligence work) may involve the same methods of collation, but with a particular focus on ensuring that information is structured to allow "link analysis" to be conducted. Criminal-pattern analysis will normally involve the collection of large amounts of data and the collation of this into relevant categories in relational databases. Collation is particularly important when there are multiple sources relating to the same event or topic. If, for example, a dissident Irish Republican

group claimed to have conducted a bomb attack targeting a British company in Northern Ireland, it would be advisable for analysts to collate information relating to other attacks conducted by that group, their statements of intent, and their capability and strength. This information could then be analyzed to establish not only the validity of the claim of responsibility, but also the likelihood of further attacks targeting the company, and whether any mitigating measures needed to be put in place.

INTELLIGENCE ANALYSIS IN THE CORPORATE SECTOR

Johnston (2003), a postdoctoral research fellow at the CIA Center for the Study of Intelligence, analyzed a large proportion of the literature on IA in order to establish the key components of analysis. He noted that the practice can be best understood as a "socio-cognitive process by which a variety of methods are used to reduce a complex issue into a set of simpler issues." Once the smaller issues have been "solved," a picture of the complex issue can be built. Davis (1997), formerly of the CIA's Directorate of Intelligence, asserts a number of objectives for IA in the government sector. These are equally applicable in the corporate world. He asserts that a valued analytical product is one that highlights:

- Opportunities and dangers for organization interests, particularly unexpected developments that may require organization reaction
- The objectives, motives, strengths, and vulnerabilities of hostile actors
- Sources of potential leverage over these and other actors
- Tactical alternatives for advancing organizational goals

As discussed in Section 1, low-probability but high-impact events are of particular importance to analysts, especially in terms of identifying triggers, drivers, warnings, and indicators.

THE ROLE OF THE ANALYST

Intelligence analysts sit at the heart of the intelligence analysis process, which is ultimately a human endeavor conducted by an individual or group. It is their role to deconstruct information into its component parts; apply critical thinking and analytical techniques to these components, looking for links and patterns, anomalies and indicators; and

then construct hypotheses that can be critically tested in order to arrive at conclusions or assessments that indicate the probability of certain events taking place. Davis (1997) notes that since IA is inherently a psychological process open to the flaws of the human mind, analysts should be self-conscious about their reasoning process, in the sense of thinking about *how* they make their judgments and reach conclusions, not just about these judgments and conclusions themselves (see also Heuer 2010).

ENSURING CREDIBILITY AND ACCESS

In order for IA to remain relevant, analysts need to maintain credibility within the organizational environment. An analyst must have authority to speak on critical issues. This is achieved via the demonstration of in-depth knowledge and substantial expertise, by cutting to the heart of an issue, and by clarifying its complexities. Unimportant factual information should be excluded. The assumption and reasoning that drives arguments must be made clear, particularly when dealing with uncertainty (Davis 1997). In the corporate world specifically, analysts need to win over the support of senior decision makers, normally members of the executive board. Credibility is won and lost during crisis events that have a major bearing on employee safety or the markets. During the 2013 North Korean crisis, intelligence analysts could have won the support of their stakeholders by producing a sharp, focused assessment of the likelihood that North Korea would provoke a military attack. This would have involved thorough analysis of patterns of previous activity and study of the internal regime dynamic between the Kim family and the military. Analysts may not have been able specifically to predict the outcome of the situation, but key drivers could have been identified and indicators pointed to that would suggest that events were developing in a certain direction. As well as benefiting the company, an impressive piece of analysis that enabled the board to improve their decision making at a critical time would more than likely leave them hungry for further intelligence product and increase the chances of financial investment in the intelligence machinery.

ANALYTICAL TECHNIQUES AND THOUGHT PROCESSES

At its essence, intelligence analysis involves the development of inferences and the creation of hypotheses. According to the *Oxford English Dictionary*,

an inference is "a conclusion reached on the basis of evidence and/or reasoning," while a hypothesis is a "proposed explanation made on the basis of limited evidence as a starting point for further investigation."

Inference development: In intelligence analysis, chains of inferences are developed that link evidence to a hypothesis. These form the basis for an argument. Analysts take known facts and assumptions and extrapolate these into a conclusion about future possible scenarios. This is a form of *deductive* reasoning. The analyst transitions from statements of fact to a position of assumption. The following example illustrates the point: All Wamanian terrorists have a tattoo of a red AK-47 rifle on their right shoulder; Victor has this tattoo on his shoulder; and therefore Victor is a Wamanian terrorist. Both premises are true, therefore the inference is valid. This differs from *inductive reasoning*, where an analyst starts with assumptions and from these moves to making an assertion of fact. For example, the red criminal group and the black criminal group are both affiliated with the white criminal gang. The red criminal group commits cyber-crime on behalf of the white criminal gang; therefore, the black criminal gang also commits cyber-crime. Although the two premises are not false, a huge number of variables must be considered before it can be asserted that the black criminal gang commits cyber-crime. Considering these two examples shows how inductive reasoning is generally considered weaker than deductive reasoning, and the analyst should strive toward the clarity of the latter where possible (Moore 2007; Omand 2010).

Hypothesis formulation: A hypothesis is an explanation of an event that has not yet proven to be true but has been built around evidence and is testable. It can be described as the best educated guess of an analyst based on reasoning and observation of the information available. In its most complete form, it will be written definitively as a statement; be based on both observation and knowledge; be testable and falsifiable; make clear predictions; and contain both a dependent variable (the phenomenon being explained) and an independent variable (the factor that does the explaining). Hypothesis generation and testing, through analysis of further evidence, is pretty much the key task for analysts. Along these lines, Heuer (2010), as a well-known veteran of the CIA Directorate of Intelligence, advocates following the scientific method during IA (see Figure 9.2).

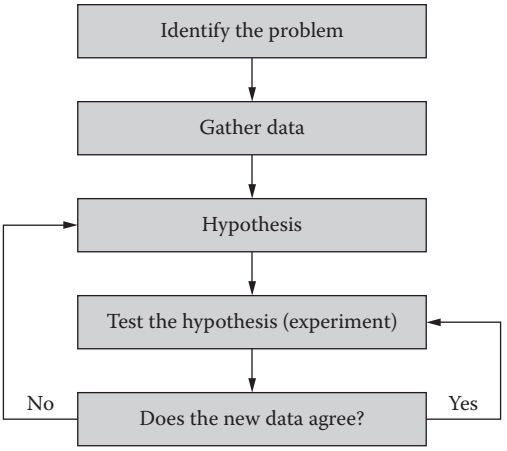

Figure 9.2 The scientific method. (Source: Wikimedia Commons.)

This requires that once hypotheses are generated, they must be systematically evaluated with the intent to try and disprove rather than confirm them. This is an uncomfortable process for analysts, but one that helps overcome the natural human desire to jump upon and seize firmly to an immediate favorite solution. The eventual conclusion is the result that best fits the data.

Heuer (2010) also suggests how hypotheses can be generated and analyzed using multiple methods:

- *Situational logic*: This is perhaps the most common mode of operation for analysts. The starting point is a consideration of the core elements of a current situation. It is regarded to be one of a kind and thus should be seen in terms of its own logic, rather than through comparison with other situations. The analyst seeks to develop a plausible narrative by identifying the logical antecedents of a situation, in terms of cause and effect. The criticisms of this approach are firstly that it assumes that understanding the values and assumptions of threat actors or situational players is possible; and secondly, that it fails to utilize theoretical knowledge gleaned from the study of similar phenomena elsewhere. For example, by focusing purely on the causes of unrest in X country, an analyst may neglect the underlying factors at play across a region. During

the Arab Spring, there were certainly unique factors at play in each country that had a strong bearing on the development of revolutions. However, there were also undoubtedly deeper, more regional drivers such as political repression and rising food prices, and social media acted as a catalyst. In practice, all aspects needed to be considered—relying on judgment on the part of the analysts and bringing their wider experience to the table.

- *Theoretical reasoning*: Theories are generalizations based on the study of multiple examples of the same phenomenon. They assert that when certain conditions arise, other conditions will logically follow with a high degree of probability or even certainty. The strength of a theoretical approach is that it economizes thought and allows for the making of quick judgments. The weaknesses are that they usually cannot specify a time frame during which something will occur, and there may be subtle differences between two situations that render the theory inaccurate.
- *Comparison with historical situations*: This approach involves the comparison of current situations with historical precedents either in the same circumstances/area, or of related events in other similar circumstances/areas. The idea is that the historical precedent may fill gaps in the understanding of the present situation. The weaknesses of this approach are that historical precedents may be so powerfully imprinted on the memory that they condition perception of the present entirely through its similarity to the past event. This is a form of "reasoning by analogy" often favored by politicians. Analysts normally have a greater depth of knowledge about a situation and so are likely to perceive the differences as well as similarities of a situation. The influence of historical comparison analysis could clearly be seen in early debates about whether Western nations should respond militarily to the Syrian regime's alleged use of chemical weapons on members of the Syrian population in late 2013. There was much talk about the similarities with the situation in Iraq, which degenerated into full-blown sectarian conflict after the deposing of Saddam Hussein's regime. There was little mention of key differences between the two situations.
- *Data immersion*: Sometimes analysts suggest that the best approach is simply to fully immerse yourself in the data without trying to fit it into preconceived patterns. It is argued that eventually a pattern,

answer, or explanation will emerge, and then the analyst must go back to the data to check how well it supports this new judgment. According to this view, an analyst must suppress preheld opinions and only be guided by "the facts." This is, however, a false representation of how analysis works. There is no "truth" that facts speak for themselves; they will always be contextual and filtered through an analyst's perceptions, whether consciously or not.

- *Data-driven analysis*: In this form of analysis, accuracy depends in large part on the accuracy and completeness of the available data. Even if the analytical model is correct and correctly applied to the data, the results will be skewed if the data are not representative. In crime-pattern analysis in the telecoms industry, for example, if the data collected on cable theft are not complete or adequately representative, this will provide a skewed picture of where crime is most likely. This will lead to inadequate distribution of resources to counter the threat, with criminals continuing to exploit knowledge gaps.
- *Concept-driven analysis*: This form of analysis is as much dependent on the conceptual framework employed as the data itself. If there is no agreed-upon analytical schema within an intelligence team, analysts are largely left to their own devices. They will interpret the information using their own mental models, which are not necessarily representative of a consensus view. This means that different analysts examining the same data might reach different conclusions (or the same conclusions but for different reasons). Information that fits with an analyst's perception is likely to be processed easily if it reinforces existing beliefs, as the mind seeks consistency. Inconsistent information is likely to be inaccurately overlooked or rationalized to fit existing beliefs.
- *Mosaic theory*: This theory suggests that as pieces of a mosaic or jigsaw puzzle are collected, eventually a picture of reality becomes apparent. All information is collected on the basis that one never knows when that information will become useful, and it is not immediately evaluated as part of a perceived larger picture. Although technically devoid of bias, simple cognitive psychology suggests that intelligence analysis does not normally work this way. Analysts typically develop a picture first and then choose pieces to fit this; such a process is more or less inevitable, so mechanisms must be worked up to counter this.

Certain analytical techniques warrant a subset of their own:

- *Link analysis*: Although this technique has been around for decades, its importance has increased dramatically in recent decades due to the proliferation of (cost-effective) data mapping and analysis technologies. These enable the drawing of far more complex networks than was possible using pen and paper alone (or, in the later "pre-technology" age, sticky notes, pins and wool, and a *very* large wall). Link analysis is critical to target-centric analysis. Humans are inherently social creatures that crave interaction, so when considering potential threat actors, it is important to consider their social and professional networks to build a picture of how they operate. Link analysis involves the decomposition and understanding of functional and behavioral relationships between people, places, objects, and events. Powerful software tools interrogate relational databases to generate visualizations of the structures of networks and the relationships between adversaries and events. Once these relationships are understood, one is better placed to draw inferences and generate hypotheses about how events have taken place. In its simplest form, network analysis can involve relationship matrixes. In more complex forms, spider diagrams are created that highlight key "nodes," or important connections. These are likely to be major "influencers" and worthy of extra attention via targeted intelligence operations or law enforcement interdiction. Even when databases do not contain complete information, link analysis can assist in the generation of hypotheses to fill the gaps.
- *Interpreting new information*: In general, once an experienced analyst has the minimum information needed to make sound judgments, obtaining additional information does not improve the accuracy of their estimates. There is a risk that new information that is consistent with an analyst's judgment will cause the analyst to become unduly overconfident, paying less attention to contradictory material. Heuer (2010) suggests a number of ways to deal with new information, dependent on the circumstance. In the case of *additional information about variables already included in the analysis*, he would not expect this to affect the accuracy of judgments. Sometimes new information will point to the *identification of additional variables*. This should not normally improve predictive accuracy, since the critical or linchpin variables that

determine a situation should already have been established. However, there are occasions when new information will alter judgments. This can normally be categorized in two ways. Firstly, *information concerning the value attributed to variables already included in the analysis*. This is particularly applicable to current intelligence. For example, new information may be collected that suggests an insurgent group is stronger than expected. This could alter the core threat judgment in an assessment. The second category is that of *information concerning which variables are most important and how they relate to each other*. Such information is of critical importance, since it forms part of the mental model that analysts use to categorize information. Omand (2010) suggests *Bayes' Theorem* as a rational way to calculate by how much one should alter the degree of confidence they have in a judgment (the probability that A is true) when new evidence (B) is taken into account. The conditional probability that A is true, given the new evidence B, is equal to the prior probability estimated for A before B was available, adjusted by a factor measuring how relatively likely it is that if A is really true we would have found the evidence for B. The adjusting factor is a measurement of the degree of surprise when B turns up, were A to be the case. If it was concluded that if judgment A was correct B would always be present, then B adds no additional explanation: One's confidence in A is unchanged. Alternatively, if judgment A being correct would mean that B should never be seen, but then evidence of B turns up, then logically one should no longer believe in proposition A and the factor should be zero. Most cases lie between these two extremes.

Note that Bayesian analysis, which we touched on in Section 1, is of particular use in scenario or multiple futures modeling, since as new information/probability assessments change, the effects cascade through the model. This allows a development to be modeled into the system or the drivers/circumstances leading to a particular end state to be understood (Figure 9.3).

ANALYTICAL FALLACIES AND PSYCHOLOGICAL TRAPS

Since intelligence analysis is a human endeavor, it is open to all of the psychological inadequacies and shortcuts of the mind. The human mind

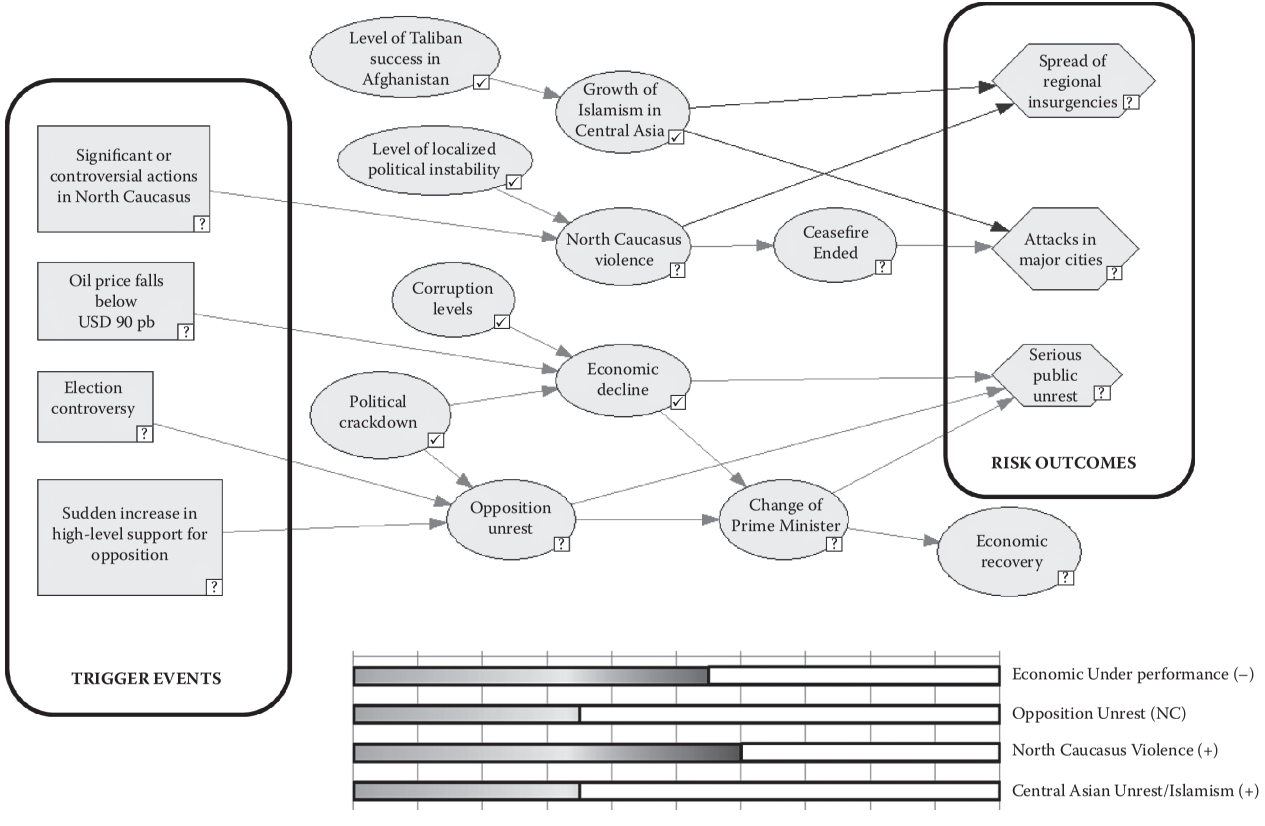

Figure 9.3 Scenario planning using Bayesian analysis, triggers, and indicators.

is ultimately poorly designed to deal with the uncertainties inherent in complex situations. People are designed to jump to rapid best-guess conclusions and take resulting action as part of our natural survival mechanism, and the fact that your ancestors had this trait is the very reason that you are now able to read this fine book. Being aware of the natural limitations helps a little when dealing with this challenge, although unfortunately they are still extremely difficult to overcome, even for the most experienced practitioner. One of the major dangers of these psychological inadequacies is that they can lead to "intelligence failure" or "surprise." Moore (2007) states that errors can be defined as "factual inaccuracies resulting from poor or missing data." Intelligence failures conversely are said to be "systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses." Jeremy Cooper similarly describes a number of pathologies that impede analysis at individual and corporate levels. It is worth recounting these here:

1. *Inefficient structure*: Structures can inhibit the sharing of information and analysis as well as cooperation.
2. *Evidence-based scientism*: This entails a prevalence of descriptive or weak explanatory intelligence to support current military options, at the expense of anticipatory intelligence.
3. *Tyranny of current intelligence*: Along the same vein, if time is constantly filled with responding to customers' immediate concerns, there is little time for longer-term research and understanding of shifting issues (something that has certainly contributed to the largest strategic intelligence failures of our time).
4. *Overemphasis on production*: Metrics of success are sometimes seen as the amount of information collected or reports generated, rather than the quality of the analysis.
5. *Overreliance on previous judgments*: Previous reports are often seen as authoritative, and at times this can lead to the retention of agreed-upon positions despite new and contradictory evidence.
6. *Neglect of research*: Reward structures often favor current reporting at the expense of longer-term research, emphasizing the "tyranny" trend.
7. *Neglect anticipatory intelligence*: Due to the information revolution, intelligence is competing with Internet journalism for the decision makers' attention. In the effort to keep up with this, at times there is a lack of predictive intelligence and failure to warn.

8. *Loss of intellectual middleware*: Frequent restructuring and downsizing in analytical staff can lead to the loss of key subject-matter experts.

The following represent common analytical pitfalls as considered by Heuer (2010) in his seminal *Psychology of Intelligence Analysis*, and also raised by Sir David Omand (2010):

- *Satisficing*: This approach involves the selection of the first explanation that appears "good enough" rather than analyzing all of the alternatives. It represents a weakness of selective perception. It means that the analyst has chosen to focus on evidence that confirms rather than disconfirms hypotheses.
- *Incrementalism*: This involves the focus on a narrow range of alternative developments that represent a marginal change while neglecting consideration of a need for dramatic change from an existing position.
- *Consensus seeking*: This approach concerns the seeking of an explanation that elicits the greatest agreement and support. The major weakness of such an approach is that potentially accurate assessments are toned down so as to reflect the lowest common denominator views.
- *Mirror imaging*: This is a key and somewhat unavoidable cognitive trap. No matter how knowledgeable and expert an analyst is in interpreting the value systems of a foreign society and culture, once the evidence runs out, there is a propensity to project one's own mindset onto the foreign culture. The danger in this circumstance is that the behavior of foreign groups or states can be seen as irrational or "not in their best interest." Such a conclusion may indicate that the analyst has projected his or her values or conceptual mindsets onto this entity.
- *Inductive fallacy*: When an analyst is seeking to prove a "desirable" (to decision makers or superiors) hypothesis, there is a risk that any new intelligence that is consistent with a preheld judgment may unjustifiably strengthen that belief. For example, in the case of the search for Iraqi weapons of mass destruction, there is a suggestion that intelligence personnel, although not overtly pressured by their political masters, were well aware that their analysis would be used to support the case for war, and they may have suspended normal analytical prudence in an effort to please them. When the convincing source Curveball seemed to provide credible intelligence of weapons development, Western intelligence agencies arguably did not put enough effort into evaluating

this source (in part due to the challenge that German intelligence refused to give access to the source, who had come to them first).

- *Received opinion*: Due to time constraints, not every point can be argued anew each time, so at some point, a level of presumed knowledge has to be reached on which fresh assessments can build upon. The risk is that inherent uncertainties regarding the initial estimate are layered over and incorporated into new assessments. New readers need to be made aware of any initial doubts that are being built upon.
- *Circular reporting*: In order for analysts to bolster their arguments, it is standard practice to try to verify and corroborate information by gathering the same or similar information from different sources. Ideally, these will be separate sources that independently provide supporting evidence. In the modern information world, however, with Internet and media sources operating close to real time, it is common for the same information or story to be rereported—often without clear attribution back to the original source. The risk is that an unwary analyst will think that they have found corroborating information when really it is simply a regurgitated story, written slightly differently.
- *Hindsight bias in evaluation*: There is a tendency for analysts to evaluate their own intelligence products or those of their colleagues in a systematically biased manner. They will often overestimate their performance. Successes will be acknowledged while failures are glossed over. Meanwhile, others may underestimate the value and quality of their work. Consumers often underestimate how much they have learned from intelligence reports; this is part of the natural human process. In postevent analysis, particularly of intelligence failures, many will normally judge that events were more readily foreseeable than they actually were.
- *Estimating probabilities*: Estimating the probability that certain events will occur is a key role for analysts. The process is often conducted in an ineffective manner, with a number of simplified rules being adopted to ease the mental burden of decision making. The *availability rule* suggests that people tend to judge the probability of events by the ease with which they can imagine instances of similar events or the number of these that they can remember. The problem is that our ability to recall events is influenced by how recently they occurred, whether we were personally involved, whether there were particularly vivid or memorable details

associated with it, and how important it seemed at the time. These factors are not related to true probability.

- *Anchoring strategy*: This suggests that people tend to pick a natural starting point for their first approximation and then adjust this figure incrementally based on new information or analysis. The initial judgment is often not adjusted enough. The initial estimate serves as a "hook" when, really, the recalculating analysis should start from scratch. Expressions of probability themselves are a major source of ambiguity. Readers often interpret them as being consistent with their own preconceptions.

AVOIDING THE PITFALLS

Analysts normally fall into these pitfalls due to time constraints or lack of conscious awareness of thought processes. Such mistakes are natural human tendencies. Such weaknesses have to be overcome through the application of tools and techniques that apply high levels of critical thinking to complex issues involving incomplete, ambiguous, or deliberately distorted information. Moore (2007) notes, however, that there is debate as to the extent to which conscious awareness of the reasoning process actually helps with analysis. One line of argument suggests that while simple choices may benefit from conscious thought, more complex issues are best left to the unconscious mind, in the sense of "deliberation without attention." The scientific thought behind this is that when the human mind is thinking consciously, it is limited to weighing up approximately seven factors, due to the survival trend noted previously, which may unjustly inflate the importance of some attributes. While it is true that the mind is limited in this sense, Moore agrees with Heuer (1999) that limits can be overcome by employing reasoning structures. For example, the number 7 rule can be overcome by subcategorization of seven top-level factors into many more. Recent intelligence failures have shown the problems brought in to play by the failure to consciously force the consideration of alternative options. Moreover, so-called intuition does not appear from nowhere; it is actually something that has been developed from experience and knowledge gleaned from past reasoning. Again, this is a powerful human survival trend that goes on at a subconscious level. As Michael LeGault notes, good decisions involve interwoven processes of emotion, observation, intuition, and critical thinking. The essential background to this is a broad base of knowledge. Such uninformed so-called *intuitive*

thinking often contributes to intelligence failures, since it fails to take into account presuppositions.

There are a number of techniques that help to mitigate human processing flaws, and which analysts and intelligence managers should seek to take into account.

Articulation and Testing of Assumptions

The identification of key *drivers* (or variables) and *linchpins* (assumptions about the drivers) is key to the analytical process. Drivers are those variables that are most likely to influence or determine the outcome of complex situations. Linchpins are the premises that hold an argument together and ensure its validity. Both should be sought, challenged, and defended prior to the writing of assessments. The clear expression and defense of assumptions is crucial, since when there is a great deal of certainty surrounding an issue, there is a higher likelihood of estimative error and divergent opinions. In order to avoid incrementalism, prior to writing formulating assessments, a search for all drivers, including potential new ones, should be conducted. All drivers that have an important impact on the issue should be identified, and links between them should be established and hierarchies of importance created. A test of how sound the linchpin assumptions are, is to ask how likely it would be for new information to adjust judgments (Davis 1997). Along similar lines, *sensitivity analysis* is a test of how sensitive your final judgments are to any changes in your major drivers. Individuals who disagree with your assumptions should be actively sought out so as to provide new perspectives and to force you to critically examine and defend your own conclusions. This is akin to a *peer review* process.

Analysis of competing hypotheses: In order to counteract the inevitability of mirror-imaging, Heuer (2010) puts forward the idea that analysts' calculations about foreign beliefs and behaviors should be treated as hypotheses to be challenged. His analysis-of-competing-hypotheses technique involves setting the hypotheses against each other in competition to see which ones survive testing. Those that cannot be disproved are subject to further testing. The process involves eight steps:

1. Identify the possible hypotheses.
2. Make a list of arguments and evidence for and against each hypothesis.

3. Prepare a matrix with hypotheses across the top and evidence down the side. Then analyze the "diagnosticity" of both arguments and evidence. That is, which components are most helpful in judging the relative likelihood that the hypotheses are true?
4. Refine the matrix by reconsidering the hypotheses and deleting evidence/arguments that have no diagnostic value.
5. Draw initial conclusions about the relative likelihood of each hypothesis. Continue to try and disprove those that seem most likely.
6. Assess how sensitive your conclusion is to the critical items of evidence. Ponder as to how inaccurate, misleading, or deceptive "evidence" would impact your conclusion.
7. Report your conclusions and list the relative likelihood of all of your hypotheses, not just the one you assess as most likely.
8. Outline future milestones for observation that could indicate whether events are developing differently than expected.

Testing hypotheses from different perspectives: A number of techniques can be used to force an analyst to think from a different perspective:

Thinking backwards involves starting with the assumption that an event has already occurred, and then establishing what would have to take place to lead to that event.

Crystal-ball analysis involves imagining that a "perfect" intelligence source has told you that your hypothesis is wrong. You must then develop a scenario to establish why your hypothesis is wrong. This forces the active disproval critical to the scientific method.

Role playing gives individuals a license to think and act differently. It stops them from being constrained by normal social or organizational conformist pressures. Role play may not result in a clear answer to a question, but it will force you through trails of thought.

Devil's advocate exercises involve somebody defending a minority view. Playing the enemy also often makes people more comfortable with confronting their colleagues and peers, and helps break down boundaries.

Utilizing memory: Differentiation in analytical performance can in large part be put down to variation in the organization of data and experience in an analyst's long-term memory. This memory

component provides continuous input into analysis in two ways: firstly, through the accessing of factual information such as background knowledge and history; and secondly by developing the schemata that the analyst uses to determine the meaning of new information. Short-term memory is the component utilized in reasoning. Its limitations can be overcome by externalizing the problem—sketching it out. Mind maps can be extremely useful in this regard, whether as a sketch on paper or in a software program (touch-screen PCs and tablets being extremely helpful in this instance).

ASSERTING CONCLUSIONS AND FORECASTING

The conclusion of a report is arguably its most important component. Conclusions should be stated boldly, with clear indications of patterns that have emerged. Analysts must display precision in conveying the level of confidence in their judgments. When there is reasonable doubt as to the quality of information, these doubts should be shared with decision makers and not hidden. Clear indications should be made as to what is still not known.

A critical component of conclusions is the forecasting of future developments and the outlining of alternative outcomes. Decision makers need such information to plan for contingencies. Statements focusing on outlook should identify the dynamics that will have the most significant impact on the development of events, i.e., "What are the drivers of a situation?" and "What drivers would have to change for the outcome to be altered?" Judgments must logically follow from the evidence and from the articulated assumptions. Where possible, probabilities should be stated in percentage form or using words of estimative probability. Factors that could lead to unexpected developments should be outlined, acting as signposts for change or triggering major shifts in direction. When addressing issues of vital organization security, analysts can at times assist in contingency planning by: firstly, b outlining all factors that could influence subsequent events; secondly, by ranking their relative importance; and thirdly, by relating these to plausible outcomes, including alternatives that may be deemed remote possibilities. Since giving precise indications of probability is tricky, the focus should shift from addressing *if* something were to happen to *how* it could happen. It is important to identify the key players and groups that have the power to determine the outcome of issues, and

then critically assess what is most likely to determine their behavior (such as family or tribal interests, personal rivalries, or institutional loyalties). By thinking backwards with the assumption that a danger has occurred, a number of plausible "how it could happen" scenarios can then be generated (Davis 1997).

Conclusions should be effectively summarized, since more often than not, consumers with limited time are only able to read short amounts of text. Nonetheless, they want to know that there is substantial, credible analysis behind the summaries in case detailed reading is necessary. If the priority interests of the customer are well known, a summary should be crafted that presents in a few lines—*what is new* and *why it is important*. When audiences are larger and more diverse, summaries should succinctly convey evidence of knowledge and expertise through the drafting of key findings and judgments. Even more so than in the main body of reports, summaries should be actionable. A side benefit to the summary approach is that the process of compressing all of the information and arguments into a summary paragraph sharpens the analyst's awareness of what is important. Key variables, cause-and-effect relationships, and argument directions become more readily apparent. Occasionally, this process will drive new insights that can be retrofitted back into the main analysis. All in all, it is better to make fewer points, but to make them well!

CONCLUSION

Analysis is often viewed as the most important part of the whole intelligence apparatus, and in many corporations, the analyst works in isolation, with the title of this role showing the weight put onto this stage. There is no doubt that analysis is one of the highest value-add stages of the intelligence cycle. However, as emphasized throughout this book, effective intelligence relies on a combination of all things being done well, and effective task allocation, requirements breakdown, research, and collation are all preconditions to truly effective analytical outputs.

As can be seen, human psychology is one of the most important things to bear in mind when conducting analysis. The task is highly demanding, requiring a combination of—to take just a few examples—confidence with acute awareness of one's own failings, extrovertedness in presentation with introverted thinking, and the need to service clients with the imperative to stand up for unpopular views.

While there are tools and approaches to help tackle the many inherent challenges, the reality is that these are difficult to overcome. Analysts have to cope with the frustration of unclear circumstances and must be comfortable with being put on the spot over their views. Producing clear and actionable conclusions and guidance from a mass of contradictory and incomplete information is stressful, and failures are almost inevitable. Of course, these will also draw far more attention than successes. The mark of a good analyst is being able to cope with this and not only survive, but also to thrive in such a challenging and demanding environment.

10

Dissemination

I apologize for writing you a long letter; I have not time to write a short one.

Blaise Pascal

CHAPTER OBJECTIVES

1. To outline the fundamental principles underlying the dissemination of intelligence material, including consideration of operational security requirements.
2. To provide guidance on the different reporting formats available—their strengths and weaknesses.
3. To provide a basic set of writing and presentation guidelines to support report production and briefing of clients.
4. To discuss how to ensure quality and track return on investment.

INTRODUCTION

Dissemination, although it comes late in the intelligence cycle, is a vital stage in the process and should not be overlooked. Ultimately, the best conclusions in the world—and the most insightful analysis—are of little use if they are overlooked. The intelligence function saying "we told you so" may be mildly satisfying, but this is a huge failure for the organization as a whole. At the heart of dissemination is the need to get the end clients'

attention and communicate things in the most suitable way. Doing this in a business environment is a particular challenge in and of itself, especially when readers may not be interested in or aware of security issues.

Often, dissemination mechanisms (formats and distribution of material) will be established in the initial stages of any project. However, a period should be set for reviewing these based on changing situations. For example, one historically accepted approach for country-risk work has been to report on each country over a set period, often biweekly. However, in practice it is more effective to allocate a periodicity to each country based on importance, velocity of change in trends, and other factors to create a more flexible system that minimizes impact on the clients' time. This is a small example of the way in which careful thinking and management by the intelligence team can help unobtrusively focus attention on what matters most.

In practice, effective dissemination comes down to clarity over recipients; effective mechanisms; and precision in presentation. All areas require constant work and attention in order to yield the most effective results, and there is little room for complacency. As ever in intelligence work, though, standard operating procedures (SOPs) are very useful aids to making the process as efficient as possible, especially in critical moments.

WHY DO WE DISSEMINATE MATERIAL?

This may seem to be a trick question, but it is actually an important thing to bear in mind. Why are we doing this at all?

Ultimately, we are seeking to achieve an *effect*. This reflects the ultimate purpose of intelligence to support the decision maker and, in so doing, to help the organization attain a goal or purpose. Sometimes this may require an extraordinary measure; indeed, this is why the Thirteen Rules of Intelligence discussed in Chapter 6 on management stress the need on occasion to be theatrical in presentation. This reflects how one may often be "selling" a difficult idea or concept to the organization. While this should never override our impartiality, it is a fact of life—and most certainly a fact of business—that people don't take away everything they hear, and they try to ignore things that are inconvenient or deemed to be impediments to desired courses of action.

With this in mind, the effects (both desirable and undesirable) that could be achieved by disseminating material always need to be considered.

This must not obscure the facts, but may well drive the classification, distribution list, and format of a piece. It is naïve to ignore this, especially in the commercial environment, and in this regard "soft power"—and potentially internal sponsorship—is once again of use.

BALANCING OPERATIONAL SECURITY

Operational security/secrecy and "need to know" is an inevitable aspect of intelligence work. As discussed under the principles of intelligence in Chapter 5, ensuring appropriate and ideally widespread access to information is highly desirable, but this raises potential vulnerabilities. An example known to the author is that of a major private bank, where a routine due-diligence investigation revealed that a potential new client was too much of a risk to take on. The relationship manager was duly informed. Unfortunately, this person was a close friend of the potential client and so chose to save face by saying that the client had been deemed unacceptable due to the findings of the intelligence team. The potential client then went to the bank and, under data protection laws, demanded access to the findings of the investigation—which created a very difficult situation, as you can probably imagine.

This is perhaps an extreme example, but it highlights the risks surrounding the release of information. Source protection is one of the most important areas to consider, and there are some useful measures to make sure that this does not become an issue. As discussed when considering the principles of intelligence, all sources of information must be adequately protected in order to preserve their ability to generate raw data and mitigate any threats they may face themselves. Source protection is not simply a function of not using their names in reporting, but also a matter of considering who receives every single report—as material can be extracted dynamically from any cumulative amount of reporting.

While corporate processes may allow for the classification of material, the desire to release material as widely as possible means that the process of *sanitization* is generally preferred as a mechanism to drive down the potential security risk posed by an intelligence product. The number of high-profile information security breaches in both the government and large corporate sectors additionally shows why this is good practice regardless of classification. Sanitization is, ultimately, the function of

the intelligence manager, but responsibility lies with all involved in the generation of material.

The following rules are suggested by the author's close colleague Steve Phelps, former British Army intelligence specialist and now CEO of Security & Intelligence Solutions Ltd:

- Write all reports as if you were an observer of the events being reported.

  For example, "A Security Intelligence Source reported that the meeting was attended by a number of senior militant leaders" can be rewritten as "A number of senior militant leaders attended the meeting."

  In the first version, it is evident that a human being who reports to security intelligence had access to information about the meeting (through a third party) or attended the meeting in person. In the second version, which is a simple statement, it is not possible to know whether the meeting was attended by a security intelligence source or one of his contacts, observed from a distance, eavesdropped upon, or compromised through loose chatter by a person who attended the meeting. The essential point is that all scenarios are possible, and therefore there is an element of doubt as to how security intelligence collected the information.
- *Never* use the word *source*.

  When grading information, sanitize the grading to avoid drawing attention to specific sources whenever possible. For example, "Information from a single, normally reliable source" can be rewritten as "Uncorroborated information that is assessed to be reliable."

  Once again, the statement is sufficiently vague to disguise where the information came from.
- *Always* reread the draft product; look at every single word and ask yourself these questions:

  1. Does this word need to be here?
  2. Does this word link to the source in any way?
  3. How can I change this in order to anonymize the source?

  For example, the following sentence—"Government Security Agencies are conducting further intelligence gathering operations in the area"—is unnecessary! It identifies that security

intelligence has a relationship with these agencies. Worse still, it is a straightforward compromise of another agency's operations, which will affect future trust and cooperation if leaked. This adds little value to the product as far as a business leader is concerned, so why include it?

- Sanitize to the appropriate level for the target audience.

  In order to reduce classifications to a level where a product can be distributed more widely, it is necessary to not only anonymize the source, but sometimes to tone down the facts of the report as well. For example:

  "Militant leader X is planning to attack facility Y with the intention of destroying it" would be classified more highly than "Militant elements are assessed to be preparing attacks against installations in area Z."

  This version removes the specifics of the raw information, namely that it is a threat emanating from leader X himself and the identity of the target. In removing these specifics, the author has generated some wriggle space in the event of a compromise. If the aim is to distribute at unclassified level, for instance on an internal webpage, the intelligence may be rewritten as follows:

  "An extant threat exists against infrastructure in region Z."

  This version further removes the specifics of the original information through avoiding reference to militants or the target area. However, it allows the document to be distributed at a lower classification and raises awareness among a wider audience.

  Of course, it may be that all variations are released at different levels to allow for maximum use to be made of the information across the business.

This is just one facet of risk management with regard to operational security. Obviously, documents pertinent to sources should be heavily protected, as should original source reports. Similarly, lists of intelligence requirements and collection plans could have a compromising role if they were to be leaked (especially with regard to M&A [mergers and acquisitions] activities, countering single-issue activism/political violence, new market entry, or where they relate to particular individuals). These rely more on information security measures, but sanitization can still occasionally be of use, where appropriate.

REPORT FORMATS

The presentation of intelligence material can take a number of forms. Some suggestions are as follows:

1. The most common remains via a *written report*. As discussed when considering types of intelligence, these will generally be either project based or used to communicate against routine criteria. These are most commonly prepared on MS Word or equivalents, although many organizations are increasingly adopting PowerPoint. Desktop publishing software may also occasionally be used, although this tends only to be for the presentation of more complex works, designed for a mass audience.
2. *Briefings* are also popular. These can be face-to-face, via teleconference, or—increasingly—by webex. Clients generally appreciate the opportunity to interact with analysts, and it is sometimes possible to impart a message more clearly in this environment.
3. *Delivery of data via web portals* is also useful, especially for more low-level information. These are commonly used for awareness purposes, for example travel security. Dashboards and SharePoint lists are very useful for showing certain topics, as are interactive maps; geospatial presentations are increasingly easy to produce, with a number of GIS programs being freely available. Using these can also add a wow factor to presentations.

Discussion of web portals brings us to a useful topic for reconsideration—the balance between push and pull factors when presenting reportage. Too much push can overwhelm clients and opens up the information security issues addressed previously; too much reliance on pull means that material may not be used by decision makers. A balance needs to be struck. Moreover, there are times when it may be important to bypass the system and present something a different way, for example when something is urgent or clearly is going to have a larger impact. In general, the Analyst and the Intelligence Manager are responsible for identifying the need for such changes.

WRITING GUIDANCE

Written products will only be read if they are timely, accurate, relevant, and actionable—and therefore they must be clear and readily accessible to the client. Key questions the writer should ask are:

- Does the title make the recipient want to open the document and read beyond the first line? The title must capture the reader's attention and be unambiguous. This goes for section headings as well, where relevant. It is therefore usually best to work on headlines once the main text is complete, since this increases the ease of formulating suitably attention-grabbing and concise titles.
- Is the report relevant to the reader? It must be clear why they should read it, due either to specific references to the company's interests or other material that places it into context.
- Will the client have time to read the report? It is surely harder to write a short report than a long one, on occasion, but the reality is that corporate readers are bombarded with material. The length must be tailored to the audience. Where possible, use an executive summary or bullets (preferably hyperlinked) to convey key messages.
- Have the 5WH—who, what, why, where, when, and how—adequately been covered? If there are gaps, have we explained these to the reader?
- Is the logical flow clear, and are ideas grouped sensibly? Is there a sensible narrative arc?

The exact format of products will vary, but in general it is good practice to adopt the approach of breaking a topic into sections based on *development(s)*, *analysis*, and *implications*. This three-stage approach is logical, considered, and reads well. It should be topped by a headline/title that should be used to summarize the issue and key implication, as discussed previously. The three-stage approach need not be explicit; it can be used in even a single paragraph in order to clearly convey meaning. For example, consider the following very basic example:

> Protestors in Kiev, Ukraine, have toppled a statue of Lenin as part of ongoing actions against the government's decision to withdraw from a potential agreement with the EU. The government is blaming the action on one of the opposition parties, and has warned of the arrest of "the vandals responsible" (*developments*). This marks an escalation in the situation in Kiev, which has seen regular larger protests at weekends, adding to a core of demonstrators at the "Euromaidan" site (*analysis*). Political buildings have tended to be the main focus of activity, and this trend is expected to continue. Corporate travelers in the city remain at low risk as long as they stay away from the main centers of protest activity. However, the possibility of confrontation

> remains, especially given the latest developments and despite the current lower-profile stance of the police and security services following serious confrontation last week (*implications*).

This is not the best piece of analysis. It is just provided as an example of how the approach can be applied. As this hopefully shows, there is an inherent logic that shows through. It also supports the logical approach from facts (the actual developments), through hypotheses (the analysis), to reach a conclusion or series of conclusions (the implications).

There are many other writing tips that can be applied:

- Naturally, writing should be to the highest standards.
- Formatting should be in line with corporate policy, or what the clients are used to; this makes it easier for them to digest the information and appears more professional.
- Brevity is absolutely essential for business leaders. Remember, reports are intended to close knowledge gaps and support decision making; they are not intended to be platforms for analysts to show off their knowledge. Verbosity is a sin!
- Active voice should be used where possible to involve the reader. To explain the difference between active and passive voice: In active voice, the subject is doing the action, whereas in passive voice, the target of the action is "promoted" to be the subject. Take the Marvin Gaye song—"I Heard It through the Grapevine" is active, but "it was heard by me through the grapevine" is passive (and much less likely to be a hit).
- Dates and times should be consistently formatted, and names consistently spelled and transliterated, to aid in knowledge-management activities and the identification of connections.
- Place names should similarly be formatted consistently. This is usually in order of geographical magnitude, e.g., village, town, district, province.
- Numbers below 10 (some say 20) should be written out in full, but can be numerical above that.
- Sentence structure is also worth considering. When reporting an event or incident, it is usually good to begin with the time/date something happened, as this creates an immediate sense of urgency and relevance. Alternatively, where providing a warning or a prediction, it can help to focus the reader by leading off with a consideration of "who," "what," "where," and "when."

- Sentence and paragraph length is also a very important consideration. No sentence should be more than two or three lines. Shorter sentences are easier to read, and effective use of punctuation helps break up more complex ideas. A useful tip is to make sure that a sentence only addresses one or two issues. Several sentences can therefore be used to convey relevant points.
- Sentences within a paragraph should generally contain information that is coherent and logically linked.
- Paragraph lengths should generally be eight to ten lines, twelve max. They should normally also be at least four lines long, usually; if less, this is generally a sign that the information conveyed can be communicated within other sections, or that it needs more amplification.
- Structural failures in writing usually reflect errors in analysis. Often this is related to the manner in which research material has been interpreted—in other words, the note-taking process. Grouping of ideas is a key part of this stage of analysis, and as the previous example shows, this is clearly evident in the final product. Time spent on this stage is often time saved, in the long run.
- Language must be kept simple; this is not a novel, a thesis, or a journalistic article.
- Business writing is professional. For example, do not use "about" as a measure of accuracy; "approximately" is better.
- Avoid jargon and military slang that is not likely to be known to the reader. Equally, overuse of abbreviations can also be confusing to the reader.
- Subjective language such as "worrying," "troubling," or "hopefully" usually detracts from the detachment of the analysis, and in some cases it can imply a political or cultural bias. A wave of terrorist attacks or sustained reputational onslaught by activist groups is, by definition, troubling for the likely audience, so this does not need to be spelled out.
- *Short-*, *medium-*, and *long-term* are meaningless modifiers without context. It is best to be precise. Similarly, avoid saying things like "at the forthcoming [event]," since this prompts "what and when" questions. Including this information in a clear fashion is a key part of what intelligence analysis can offer.
- Be aware of verbal tense. If this is wrong, the writing can convey meaning inadvertently.

- Make maximum use of diagrams, especially maps. That said, always ensure that these make sense and are not just included for the sake of it.
- Finally—be aware of repetition. This is all too easy when considering a run of similar topics, or writing day after day, and offers a real "jar" to the reader.

VERBAL TENSE

Verbal tense is the key to establishing the status of an activity, event, or threat. It is something that is often misunderstood. Steve Phelps of S&I Solutions recommends that analysts ask themselves the following questions when considering clear use of language:

- Is the action ongoing? If yes, then the verb must be in the *present continuous* tense, e.g., "The militant leader is threatening to…"
- Is the action in the past and completed? If so, then the tense should be the *simple past*, e.g., "Militants threatened to…"
- Is the action in the past but interrupted while underway? Then use the *past continuous* tense, e.g., "The militant leader was threatening to…"
- Did the action occur at an unspecified time in the past and was completed? Then use the *present perfect* tense, e.g., "Militants have threatened to…"
- Was the action started in the past and still underway? Then use the *present perfect continuous* tense, e.g., "Militants have been threatening to…"
- Is the action going to happen in the future? Then use the *simple future* tense, e.g., "Militants will threaten to…"
- Will the action happen in the future and be underway at a fixed point in time? Then use the *future continuous* tense, e.g., "Militants will still be undergoing DDR when the amnesty timeline runs out."
- Will the event occur before a fixed point in time in the future? If so, then use the *future perfect* tense, e.g., "Militants will have adopted a new posture by the end of September."
- Is the action yet to happen but will continue up to a fixed point or event in the future? Then use the *future perfect continuous* tense, e.g., "Militants will have been engaged in the amnesty process for two months when…"

Table 10.1 Samples of imprecise language and better alternatives

Imprecise language	Better alternative
Blast (except in technical references, e.g., to blast radius)	Explosion
Bomb	IED (in most cases)
Torch	Burn, set on fire
Gun (unless referring to artillery)	Weapon, rifle, AK47, etc.
Vast/massive/huge	Be more precise
Sacked/fired	Dismissed

Imprecise Use of Language

Table 10.1 shows samples of imprecise language and better alternatives to use. Note the difference between this:

"A bomb blew up, and the massive blast devastated the surrounding area; terrorists then killed several people with guns."

And this:

"An IED detonated, damaging cars and three nearby buildings; operatives from the Islamic State of Iraq and the Levant then followed this with an assault using small arms, killing three civilians."

As discussed previously, when looking at analysis, probability is a difficult topic. Vague assessments are tempting, but these should be avoided (i.e., terms like "may happen," "cannot be ruled out," "too early to tell," "remains to be seen," "great uncertainty," "should/may/could"). Instead, it's important to be precise. Make a clear judgment call and forecast, using well-understood terms. Similarly, avoid overuse of "reportedly," "allegedly," and so on. These are normally only really suitable for describing claims being made by threat groups and corporations or governments, since to repeat them exactly would make it sound like the writer agreed with them.

In a similar fashion, another "weasel term" is saying "commentators believe" (or "many people believe"). This implies an effort to share the blame, rather than making an independent assessment.

PRESENTATION GUIDANCE

There is a historical image of the analyst as an introverted and potentially timid character. In fact, this is rarely the case; as discussed in

previous chapters, corporate analysts increasingly have to be able to network effectively and present their thoughts to (sometimes hostile) business audiences.

When called upon to deliver a verbal intelligence briefing or presentation, it is worth considering the following aspects:

- *Objectives*: What are the effects you are seeking to achieve? What do you want the audience to take away from the presentation?
- *Audience*: What does the audience already know, and what are their critical knowledge gaps? What assumptions can you make about their knowledge and level of experience? What would be condescending?
- *Structure*: How best should you structure the presentation or briefing? Is there a "routine" structure or expected format to follow? Consider top-down thinking; starting with the key line; and what makes for the best logical flow. Will linear progression be allowed, or will the audience require you to jump in and out of certain parts of the presentation?
- *Delivery*: Naturally, all normal business presentation guidelines apply equally to instances where intelligence analysts are briefing clients. A course covering these is therefore an excellent part of an analyst's personal development process.
- *Support*: Will you have a presentation displayed, or will you just speak directly to the audience? What notes (or other cues) are required? What handouts should be used (remembering potential operational security issues)?
- *Feedback*: This includes feedback from clients/follow-ups, to see what was effective, as well as continuous feedback and assessment on presentation style, techniques, and so on. No matter how good you are, you can always be better!

It's even more obvious with a presentation that maps and diagrams should be used to maximum effect. Indeed, a very common error in briefings is to include too much written information. The presentation is there to help emphasize and reinforce the key points, or show visuals that accompany the text. Ultimately, people only remember a little of what they see, but will take away the pieces that are linked with strong emotion. Therefore, just one or two slides will stick, which is another reason to put time into considering the aim/desired outcomes of the presentation (in terms of policy) before it is made. This ensures that the key points are as clear as possible.

Given these realities of audience retention of information, people are increasingly evangelizing the "10, 20, 30" rule of PowerPoint. This suggests that a standard presentation should have 10 slides, last no more than 20 minutes, and contain no font smaller than 30 points. The reasoning is as follows:

- Ten slides matches the fact that most humans cannot comprehend and remember more than ten concepts from a single meeting/session.
- Twenty minutes is actually the optimal amount of time to plan to spend speaking in an hour-long standard session. Things never start on time, there are interruptions, and peoples' attention will start to fade well before the hour is up anyway. Planning to speak for less time allows for flexibility and more time in discussion. This also allows the presenter to relax more.
- Thirty-point font is readable and allows the key messages to stand out. The more text there is on a slide, the more likely it is that the presenter is not sure of their topic (or their facts). If this is you, make longer notes and still keep the slides clean. Reading what is on slides is counterproductive, as the audience soon figures this out and reads ahead of you, which breaks the synchronization of ideas and visual presentation that is the key point of making a PowerPoint presentation in the first place.

It is useful to recognize that people like, and learn by, stories. Storytelling is a great presentational art. Obviously, the intelligence practitioner has to be careful not to become overemotional or show bias. However, if the story can be presented without overexaggerating or jeopardizing the truth, then this is highly likely to be something that the audience will take away. For example, in a presentation I often give on the use of social media for intelligence, I bring in some case studies that are interesting stories in their own right; these always create a great impression, and are a far better display of capability and potential than a drier recital of the facts.

Finally, remember the advice Admiral Sir John Godfrey gave back in WWII: "Intelligence is ineffective without showmanship in presentation and argument."

QUALITY ASSURANCE

Quality assurance is a vital process. The term *quality*, when applied to intelligence, really rates timeliness, accuracy, relevance, and actionability

to the reader. This therefore applies throughout the intelligence cycle, although of course quality failures will normally only become evident when a product fails to meet the clients' needs. This reflects the ultimate quality assurance point: Are people acting effectively on the product to prevent incidents, protect and prepare the organization, and drive profits? If so, then things must be going reasonably well! However, as discussed previously, there are always improvements to be made. We are dealing with uncertainty and inherent imperfection, so tweaking, adjusting, and learning are all constant.

The following points are not exhaustive, but are designed to provide some basic guidance and stimulate thinking about what would best suit the reader's organization. Again, many apply throughout the intelligence cycle, and so the adoption of best practices (as discussed in the previous chapters) is still one of the best inherent aids to quality. One of the most important points is embracing openness and getting used to being able to "show you're working" when challenged. Assumptions and conclusions should be well documented to allow for future lessons-learned exercises to be undertaken, and to ensure that changes in the environment that may nullify these points are identified and taken into account.

Within the intelligence development process, the most basic form of quality assurance is the "four eyes" approach, where all work is edited/checked/discussed before going out. This allows the opportunity for points of view to be challenged, as well as the written quality to be checked, and potential accidental errors (all too common when working under pressure) to be picked up on. Consistency in proofing/editing can help make use of the amazing human brain to spot connections and improve the overall quality of output.

To inform internal quality control, clients should be encouraged to provide feedback regularly. It is incumbent on the team to make this as easy as possible; the rise of social media use inside an organization may be making this easier, with the option potentially to "like" posts or reports of interest—a good metric! Indeed, for my mainstream media posts on sites such as the Huff Post and al-Jazeera, the level of engagement, commentary, likes, and forwards is a useful guide as to how interesting people have found the content. The feedback can also be great in correcting errors or clearing up any confusion.

This is of course still rare with intelligence product. However, internal e-mail systems may allow for a system of rating a report very simply by clicking a radio button at the end of the mail. More simply, all of my

own firm's reports always include a contact e-mail to provide feedback to, which is hyperlinked and easy to open on mobile devices.

Of course, engagement with clients offers the best possible feedback, but this is a scarce commodity that should not be overused. For commercial suppliers, there is one fantastic indicator, which is whether people are willing to spend money on your services! Internally this is harder to gauge, but satisfaction surveys and the like can be telling and useful. Even the level of responsiveness is important to note, as this shows how important people consider it is to reply to you.

Where feedback is received, it is important to engage with this in a responsible fashion, and to show what actions you have taken as a result. It should also be logged. Sometimes the fiercest critic turns out to be your best client, and even "negative" engagement can be turned to advantage as a result of careful handling. For example, being robust and prepared to show why you reached a certain conclusion—which may challenge established perceptions—could in fact increase a particular client's respect for the team, once they realize the capability that is on offer.

You might also consider a process of peer review. This entails having someone with good knowledge look at your product and provide an assessment. This ties closely to the idea of an intelligence audit, which would examine not only the product, but also the whole structure to see if there were ways in which things could be improved, as these may be unclear to those who are too busy "fighting the battle." Moreover, this allows the integration of benchmarking against other, similar firms—sometimes helping to support an internal business case or showing that more resources are required in order to deliver greater benefits.

There is much more to quality assurance, but these points—combined with the best practice examples throughout this book—should help begin to steer you on the way, at least as regards the quality of the product.

SHOWING RETURN ON INVESTMENT

Showing ROI is one of the trickiest aspects of operating a corporate security intelligence function. Indeed, the entire corporate security department faces something of the same challenge. A particular problem is that if the job is done well, all risks are successfully mitigated, and then people wonder why they are spending so much money on a security/intelligence product! This complacency can also set in after a period of relative calm, and despite warnings evident in the wider environment.

The clearest possible example of intelligence's worth is, regrettably, when something is warned of; no action is taken; and a negative consequence results. For example, one could argue that the warnings of a likely jihadist attack on the World Trade Center in New York City before 1993 clearly showed the value of an intelligence-led approach, which—if listened to—would have saved several lives.

Taking this a step further is the case where a situation materializes, but mitigation has been taken as a result of an intelligence warning. To look at the WTC once more, after 1993, the chief security officer of Morgan Stanley proposed that a further attack was likely, with aviation being the probable vector. He wished to relocate as a result, but this was not practicable. Instead, he was given increased authority to carry out evacuation training and drills. In the event, this saved many, many lives of people from that firm on September 11, 2001. The value of that warning was, again, clearly recognizable.

Of course, sometimes things may be predicted but not develop. This may be due to external action outside the control of the company or beyond the ability of the team to have foreseen it. If so, understanding this can show that the warning was itself correct and therefore valuable, even though the risk was eventually mitigated.

All of these scenarios represent "wins" for the intelligence team. One way to monetize this is to show the value of assets protected or saved. This is not always obvious or easy (what value on a human life?), but some sort of metric can be developed.

The hit rate on intelligence of this kind need not be high. I once warned clients of a possible plot to strike targets in Pakistan, with the clear potential to affect Westerners traveling to Islamabad. The report was unconfirmed, but we made sensible recommendations to recipients in terms of risk factors to avoid, basic precautions, and so on. In the end, the attack materialized, unfortunately leading to several deaths at a UN building. One of the clients had had senior staff in the city at the time who had followed the precautions given; they had greatly appreciated the advice and warning, which reinforced their faith in the security department. My client in turn stated that this one warning had more than justified their expenditure, indicating that "get one in ten of those calls right and that's more than enough." It is reassuring to know that these small successes are noticed. This can otherwise be a thankless job sometimes, with failures being more remembered than successes due to the consequences, as we've often discussed in this book.

Ultimately, a system of key performance indicators (KPIs) and other metrics can be instigated to track progress. This can include more basic things than measurements of lives or investment saved; instead, these can be linked to output, customer satisfaction, and achieving certain work targets. Setting these up is a business function that will rely to some extent on the organization's existing environment and appetite, and I know many intelligence teams that would rather not have these, but are forced to do so! As with all corporate management practices, they can be turned to advantage if used sensibly and constructively, so putting thought into this area and not being too bullish is important.

CONCLUSION

Dissemination is more complex than it may at first appear. It includes many complicated functions, such as defining products to suit the changing needs of clients; managing the output and communication process; ensuring that things flow smoothly; guaranteeing quality in an imperfect environment; and continually feeding back and adjusting people, processes, and technology.

Ultimately, the only success measure is whether or not people use the output. It must therefore be timely, accurate, relevant to their needs, and actionable. Clarity and brevity are important aspects of this, and analysts in particular need to understand their audience. Writing in too academic or journalistic a style, or presenting didactically or condescendingly to a senior audience, is a sure way to lose face—and vital influence. In this day and age, it is vitally important not to waste corporate readers' time.

Section III

Practice

11

Operational Models

CHAPTER OBJECTIVES

1. To discuss why it is useful to have a model of intelligence to help guide structures, processes, and the deployment of resources.
2. To introduce a simple security intelligence model, applicable to any scale of deployment.
3. To discuss aspects of a common dedicated countercrime model (the National Intelligence Model).

INTRODUCTION

Having talked through the reasons why we should (and, indeed, must) have corporate security intelligence and addressed the theory, it now seems only fair to help the reader work out how to put this into practice. The purpose of this chapter is therefore to talk through a couple of useful models that work in quite different ways. In reality, all operational models will differ, and this is all to the good, as the doctrine should be applied to the task rather than the other way around. However, they also all have common elements, and having a model provides a degree of assurance that everything is in fairly good shape and that nothing important has been forgotten.

A CORPORATE SOLUTION: THE SECURITY INTELLIGENCE DECISION ADVANTAGE RESEARCH MODEL (SIDEARM)

Remember the piece earlier in the book, where we talked about the need to hook people on occasion and be theatrical in order to get a point across? I freely admit that the name of this model reflects that imperative. Joking aside, SIDeARM is designed to be the convenient safety net to help any size organization seeking to implement intelligence in an effective and efficient fashion. Put simply, it incorporates all the theory we have discussed, and quite a bit of best practice, in order to present a template to follow. It does not mandate particular products, unlike the National Intelligence Model for policing (see discussion later in this chapter). Rather, it lays out a framework and approach within which cohesive intelligence outputs can be delivered.

SIDeARM, as an approach, can be embedded in any intelligence team. Even one person for whom intelligence consumes just a fraction of their time can make use of it. In effect, it helps ensure that what is being produced is intelligence rather than just information, and it does so by bringing in a structured and disciplined approach.

WHAT DOES SIDeARM CONSIST OF?

SIDeARM closely echoes the modified version of the intelligence cycle introduced in Chapter 5, the "hub and axle" or "engine and driveshaft" model. It is therefore broken down under the various functions within the cycle. Again, even just one person can do all of these, especially if they are using the model as a guide to help them remember which "hat" they should be wearing at which time! The SIDeARM model is shown in Figure 11.1. The key point of the model is the structural and architectural aspects it suggests. It's easiest to understand this by briefly looking at each stage in the cycle. (Note that templates for each of the supporting functions mentioned are available on the website accompanying this book.)

Management

Three are four important things to consider under the Management heading. These are:

- *Mission and vision statement*: It is important to define what, exactly, the function is meant to be doing. This helps to set the tone and

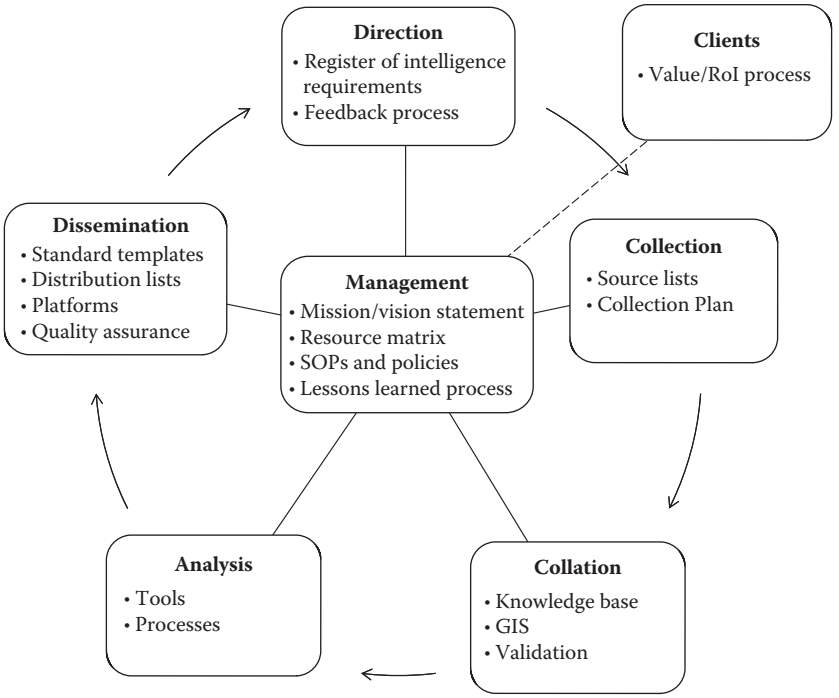

Figure 11.1 SIDeARM model.

keeps all involved (including external stakeholders) focused on what is trying to be achieved.

- *Resource matrix*: This can vary, but the aim is to have clarity on what resources are available at what time, and what intelligence requirements (IRs) they are allocated to. This is usually kept as a spreadsheet by the manager, although if you have access to SharePoint, a combination of tasks and a calendar are also useful for keeping track.
- *SOPs and policies*: The exact number of these will vary; where possible, corporate policies should be distilled for relevant points or otherwise leveraged. Often, effort here revolves around understanding what exactly corporate policies dictate and then communicating these (some people refer to this as the "BS filter"). The minimum required is probably operations security (OPSEC), research guidance, process diagrams, and writing standardization

guidance. However, it is good to check against the list provided earlier in the book for an exhaustive assessment of what *may* be included!

- *Lessons learned and blue-sky process*: These are strictly different things, but they are to some extent related as management functions. Blue sky challenges the current assumptions and is often overlooked, since it is a "nice to have" function. However, it is very important in terms of countering those pesky high-impact/low-probability events. Meanwhile, lessons learned are more related to dissecting and analyzing failures (part and parcel of intelligence work). Both together are however about boosting long-term effectiveness and are integral to a healthy system.

Direction

Direction is both the start and end point of the intelligence cycle (if a cycle really has as such, which some would argue it doesn't). There are two main things to consider when looking at direction:

- *Intelligence requirements register*: We have discussed at length how these are the things that energize the process. It is all too easy to let these slide. SIDeARM mandates that a register of intelligence requirements be kept. This is assigned against the resource matrix and collection plan in order to ensure that tasks are managed coherently.
- *Feedback process*: It is vital to collect feedback from clients, and there must be a formalized process for doing so. Again, there is no mandated standard for these; rather, the process must be given consideration, and adequate arrangements be made. This includes ensuring that the consequences of feedback are acted upon and communicated both to the team and the client from whom feedback was elicited.

Collection

The collection process similarly has two main enabling documents:

- *Source lists*: These are highly confidential if they refer to human sources, open-source lists less so. Source lists are highly dynamic and require active management, so SIDeARM recommends that they be reviewed as a matter of routine by the intelligence

manager. This prevents lists of dead links and ensures that new sources are being identified and added. Note that the resource plan may identify that there are gaps in sources that need to be filled. This should also be reflected in the source lists themselves, as a reminder/prompt to the collectors. For maximum effectiveness, though, this should clearly be issued to someone as a task.

- *Collection plan*: This brings the source list and IRs to life, allocating resources and sources to objectives. As this implies, there are tight linkages between the various documents that have been established to guide and shape activity. This is a critical document, and yet it is so often overlooked.

Collation

The main aim of collation is to ensure that information can readily be accessed and connected as part of analysis. "Joining the dots" is a critical feature of intelligence work, after all. Time invested here is vital.

- A key feature is the *knowledge base*. This can take many forms: shared drives, SharePoint libraries, cards in a box—technology is making this ever simpler, and yet also adding layers of complexity. Ultimately, this is an archive space where documents and other material can be stored and indexed. This can include in noting programs such as OneNote and Evernote. All knowledge/information should, where possible, be kept inside one "wrapper" in order to help OPSEC and also allow for ready searching across the entire data/knowledge set.
- *GIS* (geographical information systems) are also critical. SIDeARM breaks these out, as this is a factor that is often forgotten until someone realizes that a map would be useful—often when a database is already huge and geo-coding it would take months. Work this in from the start where possible; it's time well spent, as visualization is incredibly useful. Obviously this is dependent on the circumstances, but geographic and temporal analysis has many uses.
- *Data validation*: As discussed in Chapter 8 on collation, a key part of data retrieval comes from having common standards. Effective data entry and consistent capture require attention, guidance, and discipline, else they will break down. Guidelines must therefore

be clear, and the process of validation must not be allowed to be eclipsed by timing issues, overload, etc. To do so is to put in place short-term gain at the expense of long-term pain and inefficiency.

Analysis

Effective analysis relies to a large extent on the individual's mindset and the processes in place, which allow the analyst to overcome inherent limitations. Support is therefore provided under SIDeARM in two areas;

- *Tools*: This can include a compendium of techniques, reference guides, and of course technology, particularly as regards data visualization. This is becoming more and more important with the rise in the ability to capture and store huge amounts of data.
- *Processes*: Sound analytical processes must be embedded and to some extent come from careful structuring, allowing people to have the time and space to do the task properly, and the access to support where required. The traps and pitfalls were discussed at length in earlier chapters; time spent on considering analytical processes will greatly help the quality of the output.

Dissemination

The dissemination stage is when material gets sent to the client. Timeliness and accuracy are important at this stage; relevancy and "actionability" should have been covered by having good IRs, sources, and collection plans. Saving time on distribution is therefore essential. Moreover, OPSEC is a big issue here, as product readily links. There are therefore a number of things to consider.

- *Standard templates*: These help speed up distribution and help clients absorb information quickly and easily. They should not constantly change, but there should be efforts periodically to tweak these based on feedback to improve usability both for analysts and for clients.
- *Distribution lists*: Again, contact should be quick and easy. It is pointless putting in all this work throughout the intelligence cycle to then fail to get it to clients due to not having their address at hand!

- *Platforms*: Consider what other platforms and vectors can be used. There almost certainly needs to be an archive available to clients to put reports into context. Can you make greater use of this to support wider distribution of information? (Push vs. pull again.)
- *Quality assurance*: This is often underrated. As a minimum, I recommend "four eyes" and proofing where possible. That said, this shouldn't unduly affect timeliness, at least not for critical information.

Clients

Much client input is captured through the direction–feedback process. However there is one discrete input.

- *RoI/Value process*: This requires a different sort of engagement with clients to try and put a financial value on the service. This can be related to key performance indicators (KPIs), where appropriate, or use a "real recognized value saved" system, as previously discussed.

Other Factors

Although not broken out here, SIDeARM also highlights enabling structures of technology and infrastructure. These are not mandated, but rather should be applied and considered by the manager throughout.

COUNTERING CRIME: THE NATIONAL INTELLIGENCE MODEL (NIM)

It can be seen from the previous section that SIDeARM is a conceptual model for a healthy functioning system. It does not mandate particular standards; rather, it recommends a series of components that together make for an effectively managed whole.

For contrast, let's now look at the National Intelligence Model (NIM), launched by the UK National Criminal Intelligence Service (NCIS) and adopted by the Association of Chief Police Officers (ACPO) in 2000, and set out a national model for an intelligence-led approach to policing. For the purpose of NIM, intelligence refers to "information that is subject

to a defined evaluation and risk assessment process in order to assist with police decision making," with the model setting out a standard for all UK police forces in order to ensure that policing practices are guided by fully researched, developed, and analyzed intelligence to provide strategic direction and support tactical and operational decision making. Nonetheless, the model at its core does not aim at providing an in-depth technical guide on information management; rather, it serves as a standardized practical approach to information collection, storage, and dissemination in any security environment in accordance with set legal and ethical standards. Accordingly, its core principles can be applied in any risk management environment to accurate, timely, and ethical information and intelligence management within and between organizations.

NIM at a Glance

In its broadest form, NIM is a product-oriented service that defines a process for setting priorities and a framework in which the identified problem priorities can be solved. NIM is therefore adaptable to not only police or intelligence services, but also to any areas of business requiring a guided, informed, and standardized approach to risk management.

The model defines three levels of operational practice:

Local: Managing a smaller geographical area
Regional: Focusing on issues affecting more than one local area, which may require cooperation and an interagency approach
National or *international*: May often include cross-border impact and require the management of issues that also combine the first two levels

These levels of operational practice are not necessarily interdependent; rather, the operational practices work codependently, dependent on each level's requirements. The mechanisms behind the exchange and sharing of intelligence are therefore crucial to ensure effectiveness and maintain consistency of intelligence products that can be applied to:

- Crime and criminality at all levels, including perpetrators
- Non-crime-related issues, such as reputational risks and deviation from code of practices
- Interagency partnerships
- National and international cooperation and coordination

With the main goal of the National Intelligence Model being to ensure that any actions steering decision making are based on researched and analyzed information, NIM provides a standardized approach to this by ensuring:

- Operational security and effectiveness
- An informed approach to identification of threats, risks, and key priorities
- Inter- and intra-agency consistency
- Informed resource allocation (financial and human)
- Greater compliance with legislation (e.g., human rights, RIPA)

NIM in Practice

The National Intelligence Model is designed to put intelligence at the front of every action—to steer and guide the direction of decision making on operational, tactical, and strategic levels. To achieve this, the approach focuses on four intelligence products (which are produced at each of the three levels of operational practice outlined previously):

Strategic assessment: A document produced by intelligence units to provide a wider overview and predictions of a situation locally, regionally, or nationally over a six-month period. This document provides a foundation for a Strategic Tasking and Coordinating Group (T&CG), which typically consists of senior decision makers and stakeholders. Based on the strategic assessment, the group also sets out the *control strategy* and *intelligence requirements* for the three levels of operational practice for the forthcoming period. This provides direction as to what information and intelligence should be collected in relation to the set priorities and other emerging issues in order to identify further trends and patterns that may pose an ongoing threat or constitute immediate or long-term risks.

Tactical assessment: A document that outlines predictions to direct tactical priorities at a more immediate time frame (every two weeks). Also produced by the intelligence function at all levels, the document is reviewed by the Tactical T&CG. The outcomes of the meeting and the tactical directions are then reviewed at the next Tactical T&CG, allowing for the evaluation of measures taken and identifying areas for improvement.

Problem profile: This is typically commissioned by the Tactical T&CG to identify the scale of a particular issue within any of the three levels of operation in order to evaluate priorities for further direction of resources.

Target profile: This is also typically commissioned by the Tasking T&CG, focusing on a profile of suspects or offenders to identify patterns in behavior, networks, and geographical areas in order to identify areas for tactical operational priorities.

These products are supported by a guided process of information *collection*, *evaluation*, and *dissemination*, including source protection. To ensure that best practices are standardized across a range of agencies, NIM includes a set of standard guidelines, referred to as the 5×5×5 system.

The system grades the source by five letters (A to E) and the information by scores of 1 to 5, and it sets out any applicable dissemination limitations based on the sensitivity of the information and source protection in the same way (an example of a 5×5×5 sheet can be found in Figure 11.2). Although a dedicated intelligence team, often consisting of researchers and analysts, will ensure that the process is followed correctly, the information itself can be collected from an array of sources, including the public, organizational assets, and/or partner agencies. Once correctly researched, evaluated, and sanitized, this information will be used to feed the four products described here in order to identify gaps in intelligence, identify risks, direct tactical resources, and identify strategic priorities.

NIM Considered

Similar to its role in intelligence-led policing within the law enforcement sector, NIM provides a standardized guidance to intelligence management by promoting partnerships and information sharing in any security environment. The basic components of NIM can therefore be readily applicable as a standardized approach to risk management in an array of businesses in order to improve any entity's ability to mitigate risks and threats. Information management is therefore not simply a goal; it is a tool to support and enhance decision making at operational, tactical, and strategic levels.

The National Intelligence Model does not form a technical solution to risk management within a corporate security environment, but can rather serve as a guideline to a more standardized intelligence-led approach that can aid in gaining an accurate picture of the business as a

Template 1

NOT PROTECTIVELY MARKED UNTIL COMPLETED

GPMS:	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

5×5×5 Information Intelligence Report Form A

ORGANISATION AND OFFICER				DATE/TIME OF REPORT	
INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)				REPORT URN	
SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER					
SOURCE EVALUATION	**A** Always Reliable	**B** Mostly Reliable	**C** Sometimes Reliable	**D** Unreliable	**E** Untested Source
INFORMATION/ INTELLIGENCE EVALUATION	**1** Known to be true without reservation	**2** Known personally to the source but not to the person reporting	**3** Not known personally to the source but corroborated	**4** Cannot be judged	**5** Suspected to be false
REPORT					
PERSON RECORD:		**DoB:**		**NIB CRO:**	
OPERATION NAME/NUMBER:				S	I H
INTELLIGENCE UNIT ONLY					
HANDLING CODE To be completed by the evaluator on receipt and prior to entry onto the intelligence system. **To be reviewed on dissemination.**	**1** **Default:** Permits dissemination within the UK Police Service **and** to other law enforcement agencies as specified. [See guidance] ☐	**2** Permits dissemination to UK non-prosecuting parties. [Conditions apply, see guidance] ☐	**3** Permits dissemination to (non EU) foreign law enforcement agencies. [Conditions apply, see guidance] ☐	**4** Permits dissemination within originating force/agency only: Specify reasons and internal recipient(s) Review period must be set. [See guidance] ☐	**5** Permits dissemination but receiving agency to observe conditions as specified. [See guidance on risk assessment] ☐
5×5×5 REVIEWED BY: RE-EVALUATED: Yes ☐ No ☐		CROSS-REF URN:		TIME/DATE OF REVIEW:	
DISSEMINATED TO:		PERSON DISSEMINATING TIME/DATE:			
DETAILED HANDLING INSTRUCTIONS:		PUBLIC INTEREST IMMUNITY:			
INPUT ONTO AN INTELLIGENCE SYSTEM Yes ☐ No ☐					
SIGNATURE (PAPER COPY):					
GPMS:	**RESTRICTED** ☐	**CONFIDENTIAL** ☐	**SECRET** ☐		

Figure 11.2 Example of a 5 × 5 × 5 information intelligence report form. (From ACPO [2010]. With permission of the Association of Chief Police Officers, 2010.)

whole, including its capabilities, understanding the risk and threat environment, and identifying high-risk areas in order to ensure effective and efficient resource allocation against problems. Similarly, implementing a NIM-based approach does not necessarily require separate allocation of resources. A standardized intelligence-led approach will instead aid in allocation of often-limited resources: By applying the problem-solving approach, resources can be better focused at identified high-risk areas, targeting the problems through informed strategies.

With the ever-evolving risk and threats facing businesses and corporations worldwide, adoption of a standardized approach to information sharing can:

- Reduce definitional differences by following set guidelines
- Reduce duplication of efforts by appropriately documenting and storing intelligence
- Reduce duplication of efforts by sharing intelligence
- Increase cooperation and collaboration within and between organizations
- Increase operational and tactical consistency
- Increase awareness of risks impacting businesses
- Increase awareness of best practices in risk mitigation
- Increase source protection

CONCLUSION

These are two very different models, with different purposes in mind. They also approach the underlying topic in different ways. Neither is better (although I would argue that SIDeARM is more broadly applicable to corporate work than the NIM). However, both can provide guidance to someone who is looking to establish a function or who wishes to "health-check" their own function against a set of criteria. As ever, there is no right answer, and systems depend on people, process, and technology rather than just one aspect; weaknesses in one area can often be countered by strength somewhere else. That said, having the right balance of ingredients helps a lot, and architecture designed to fully support intelligence production will reward those who invest the time and effort.

12

Implementing the Function: The Intelligence Estimate

CHAPTER OBJECTIVES

1. To discuss the need for a coherent process to address the implementation—or auditing—of an intelligence function.
2. To present a sample process to implement intelligence in the corporate security environment, known as the Intelligence Estimate.
3. To discuss how to use the Intelligence Estimate to best effect.

INTRODUCTION

Section 2 explained the theory and best practices around the implementation of intelligence in the corporate security environment. As the discussion in Section 2 showed, there are many points to consider in order to make the function as effective as possible. Getting started is therefore quite a challenge, and this has presented a serious barrier to many corporate security departments looking to establish a function. As with all tasks, it is much easier when there is a template to follow, and so the following is a suggested approach. As with all such structures, it should not be slavishly followed, but rather be used as an intelligent guide to help the generation of a cohesive security intelligence capability. The aim

is to raise areas that require consideration and, ultimately, lead the user to create:

- The key documentation and processes required to support the function
- A range of potential products
- A project/implementation plan
- A business case

This process is tried and tested, and it has been used to coach a number of large corporate clients in establishing an intelligence function. It has most commonly been implemented during a two-day workshop attended by key internal stakeholders (some of whom may just attend parts). However, it has also been used successfully in a series of short sessions addressing different parts of the total problem. Again, there is no right or wrong way to use this; what is best is whatever works and suits the implementer's organization.

A SUGGESTED APPROACH: THE INTELLIGENCE ESTIMATE

The Intelligence Estimate has been created to guide the (would-be) corporate intelligence practitioner seeking to implement an internal function. Why an "estimate"? Well, it is based loosely on the structured approach used by the military to develop a plan—known as the *estimate process*. Although quite different from any actual military structure (especially the British Army's intelligence estimate, despite the name), it therefore has overtones of these processes, especially in regard to the general shape it gives to the discussion. This can perhaps best be summarized as: "What do we have to do?" "What do we have to consider?" "What do we have to do it with?" and therefore "What should we do?"

The Estimate (as it will henceforth be called) is made up of a number of top-level stages, each of which has a number of categories (Figure 12.1). These are as follows:

1. *Task analysis*, which considers what the effects of the intelligence function are intended to be
2. *Environmental analysis*, which predominantly looks at geographical factors and the whole range of potential threats

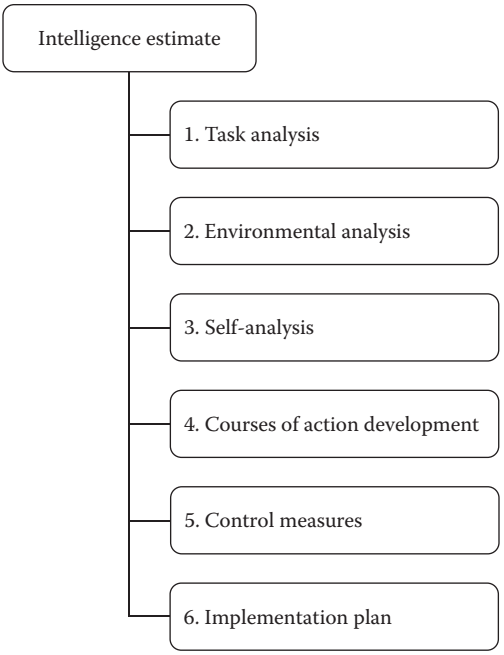

Figure 12.1 The Intelligence Estimate.

3. *Self-analysis*, which considers resources, customers, and constraints imposed by the organization
4. *Courses of action development*, which group the previous deductions in an effects/action-based structure and allows for the allocation of resources to tasks in order to identify gaps or optimal outputs
5. *Control measures*, which consider processes, procedures, and policies
6. *Implementation plan*, which supports the development of a structured project as the final output from the process

The Estimate is generally written up in a spreadsheet or table, using a three-column format. These are entitled *Factors*, *Analysis*, and *Deductions*. The factors—or topic categories—are discussed in detail in this chapter; the analysis and deductions are what those working through the estimate can divine as a result of the thought process engendered. At various stages, the deduction process will generate an *Output* that will in due course form a part of the intelligence architecture of the business, for example the Master List of Intelligence Requirements.

There are no hard and fast rules to how to make deductions from the factors; to some extent, that is the beauty of the process—it is there to stimulate thought. This is why, as much as possible, each factor or subfactor is written as a question, since this naturally prompts the reader/practitioner to start thinking in detail about the question posed. Sometimes this may stimulate lateral thinking or prompt a note relevant elsewhere, in which case this should be entered into the table as appropriate.

A good way to do this is therefore to put the list up on a projector and to type into the boxes live on screen, when working as a group (and clearly it is preferable for a number of people to share ideas when working up the intelligence architecture). Other useful items are a whiteboard and a bottomless vat of coffee! Note that from time to time, participants may also identify new factors or think of new angles that should be considered, particularly in relation to their particular organization. This is to be encouraged, and again readers are reminded that no process is truly comprehensive. While this list is a great start, it is therefore always worth reviewing the whole list of factors in advance and just considering whether any others come to mind. Additionally, project management gurus—for example, those with PRINCE2 (PRojects IN Controlled Environments) qualifications or similar—may well want to incorporate these aspects into the Estimate, or corporate guidelines may dictate a certain form of output. In these cases, readers are encouraged to tinker with the templates offered in order to get something that is as suitable as possible. To some extent, this is "task zero" at the beginning of the assignment, although this is not always strictly necessary!

TASK ANALYSIS

It is always useful to begin any complex task by considering what exactly is the ultimate aim and purpose. This helps all involved stay focused on the eventual objective and output. It also helps to ensure that tasks are clearly identified. This can include both *specified tasks* (things that are explicit in the direction given) and *implied tasks* (things that fall out as deductions). Ideally, the task would be given by higher management (e.g., the CSO) or agreed upon in advance—but of course this is not always the case.

Task analysis (Figure 12.2) also implies examination of the timeline and also allows for initial assessment of the key internal decision makers and potential clients. This is particularly useful when considering project

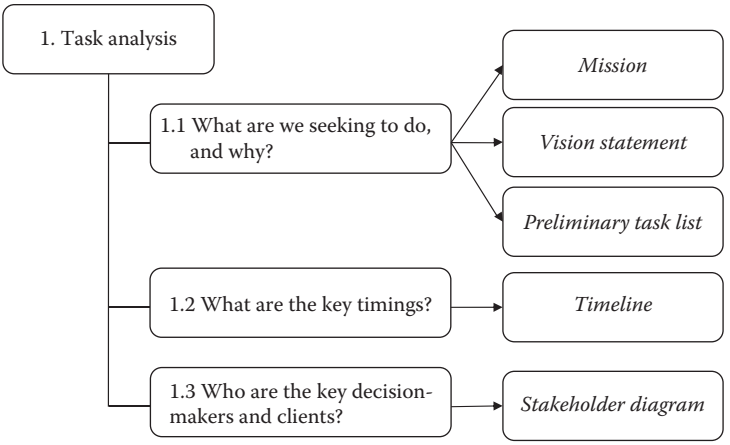

Figure 12.2 Task analysis.

implementation and success, and helps guide the "sales" process inside the organization.

Task analysis has three main areas:

What Are We Seeking To Do and Why?

This question is deceptively simple. If provided with no guidance, you can readily take some of the material presented earlier in this book, as the purpose of all corporate intelligence structures will be broadly similar! However, putting this into your own words is a critical part of the process. As mentioned earlier, this is the very first consideration, as it should ultimately underlie everything else you address. It's the unifying purpose of the whole process.

This is also a useful place to consider terminology and especially the naming of the function, as this can sometimes be contentious. The outputs from this include:

- *Mission statement*: Defining this is a part of management (see Chapters 4 and 6 for more guidance).
- *Vision statement*: Again, see Chapters 4 and 6.
- *Preliminary task list*: This is an initial "brain dump" of the things the intelligence function might be expected to achieve under the overarching mission. As mentioned previously, some may be specified, and some may be implied from the expected requirements.

What Are the Key Timings?

With any project, it is also useful to work backwards with regard to a timeline. The key requirement will probably be when you want to have something in place, often at the start of a budget year. Other timings to consider could include dates related to budget cycles, major corporate events, or meetings when the implementation of intelligence is planned to be discussed. At this stage, there should be an effort to get as much useful information as possible together onto the main output, which is the

- *Timeline*: This is a "living document" (in fact, all outputs are—they're never set in stone) that is updated as the Estimate proceeds. It is an integral part of the project's rhythm and should include internal deadlines and timings for key project milestones as these are developed. Note that a SharePoint calendar or equivalent makes for an excellent timeline, being easy to maintain and use to manage tasks.

Who Are the Key Decision Makers/Clients?

The process of stakeholder identification also never stops, particularly in larger organizations. Internal stakeholders include (but are not limited to) potential intelligence clients/consumers, potential "sponsors" or advocates for the functions, the management chain, and those who are engaged in complementary or potentially rival functions (e.g., an economic analysis or political studies unit). Discovering clients in large organizations is an almost ceaseless process, and the reality remains that intelligence teams spend significant time trying to keep up to date on their own organizations!

- Relationships are initially plotted and kept track of through the *stakeholder matrix*. This common diagram maps people on two axes, based on their awareness of the function (low to high) and an assessment of their sentiment (supportive to negative). The current location and trajectory of relationships can be mapped. This can serve as a useful "who do we need to talk to" list.

ENVIRONMENTAL ANALYSIS

Environmental analysis (Figure 12.3) covers a whole process of looking at where the organization operates, what it does, and how it goes about its

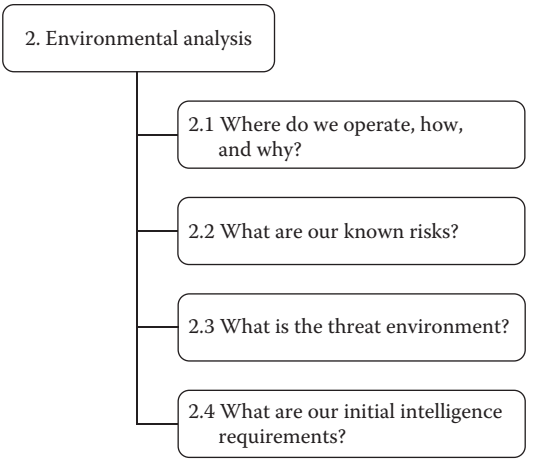

Figure 12.3 Environmental analysis.

business. This can help the intelligence team spot what is important, and it helps put a risk register (if one exists!) into context. The ultimate output from the environmental analysis process is the creation of the *master intelligence requirements* list—something that will become a core part of the intelligence process, as discussed throughout the book.

Where Do We Operate, How, and Why?

Clarity over the geographical spread of the company or organization, examining what it actually does (not always clear to those who are not directly involved in it), and coming to grips with what makes things "tick" are all essential elements of understanding the environment in which the intelligence function must operate. This helps identify what is likely to be most important to consumers of intelligence. This knowledge can principally be obtained from company sources, usually internal websites.

What Are Our Known Risks?

Organizations are likely to have at least some form of risk register; some may have many. These will often go well beyond areas where the security department has direct input. However, that is not to say that the intelligence function will not have a bearing, reinforcing the potential for the

department to gain "soft power" and influence (see Chapter 1). Moreover, gaining insight into factors driving the risks considered to be of most importance to the organization ensures that the material is highly relevant to consumers and helps drive important actions. Relevance and what one might call "actionability" are, of course, two of the cornerstones of effective intelligence—so the value of research at this stage is very high.

What Is the Threat Environment?

This presumes that those conducting the Estimate have some preexisting knowledge of the threat environment; fortunately, this is usually the case. Chapter 2 of this book provides some background and a useful checklist of aspects to consider. Some threats may be well known; others may just be identified as potential areas of concern at this stage.

At a minimum, it is worth considering the following areas/vectors:

- Country risk (politics/economics/security)
- Travel risk (where are people going and how are they viewed there?)
- Terrorism
- Single-issue violence and political activism (SIVPA)
- Cyber- and information-security issues
- Insider threats
- Fraud
- Counterfeiting/product piracy and intellectual property

What Are Our Initial Intelligence Requirements?

The process described here will very naturally lead to the creation of intelligence requirements (IRs). In fact, asking "What is the threat to our business from X?" is likely to arise very soon in the discussion! This can be integrated with an understanding of key markets, supply chain factors, relationships, and critical assets in order to present some focused questions. These can be prioritized, which may come in useful when allocating resources—there are bound to be more things that could be examined than resources available. If there aren't, then you need to readdress this stage or possibly become more of a worrier (arguably a vital component of being an analyst).

IRs are most usefully recorded in a spreadsheet, as discussed in Chapter 6.

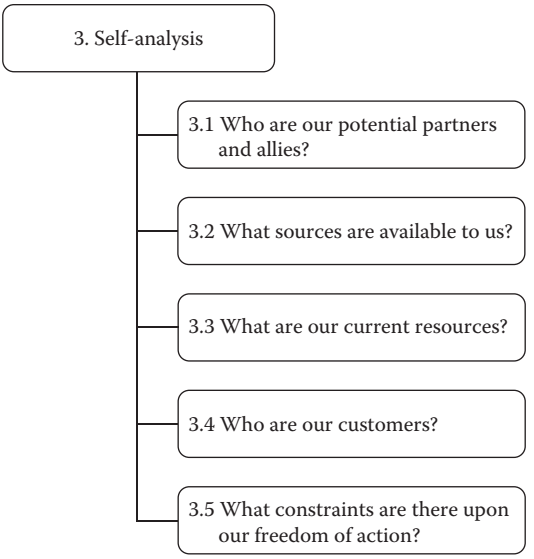

Figure 12.4 Self-analysis.

SELF-ANALYSIS

Self-analysis (Figure 12.4) is a natural extension of the previous section. However, where that focuses on threats and issues of importance, this focuses more on internal resources and the restrictions/constraints inherent in a large organization.

Who Are Our Potential Partners/Allies?

This is really the first part of source development. The aim is to start to identify partners who may be able to provide high-value material, both internally and externally.

- This is the first input on the *master source list*. As previously discussed, this is a particularly confidential document (or will be in due course)—so apply appropriate security.

What Sources Are Available to Us?

Some of these will be obvious, some less so. Apply the source categorizations discussed in Chapter 7 on intelligence collection in order to consider

all the options. It is not important to overresearch sources at this time; rather, consider the rough scope and volume of information. The work of pulling together sources is constant, and development requires sustained effort and attention, but this can follow. For now, the main effort is identifying where there are assets and where there are gaps that need to be filled.

What Are Our Current Resources?

This includes people, hardware, software, and infrastructure. These are obvious assets; don't overlook the ones that are less so, such as existing processes and policies that may make life easier. It is useful at this point to deduce the things that you may require but do not currently have access to—particularly in regard to technology.

Who Are Our Customers?

This is a natural extension of the initial stakeholder analysis, bringing into account the additional examination undertaken through stages 2 (environmental analysis) and 3 (self-analysis). The deductions can be added to the stakeholder analysis template or, at this stage, recorded under the deductions.

What Constraints Are There upon Our Freedom of Action?

Things to consider here include national and international legal issues, especially in regard to data protection and conducting investigations. Questions for the legal team should be noted in the deductions column. The analysis should also consider areas of responsibility for the security department. For example, is information security included in the department's purview? If not, will reporting on cyber issues cause conflict with other teams elsewhere in the organization?

Budget is a perennial issue, which may have been addressed under analysis of resources as discussed previously. Finally, organizational policies must also be understood; the intelligence team's standards on matters such as ethics are likely to come under intense scrutiny.

COURSES OF ACTION DEVELOPMENT

As you have by now perhaps already observed, there is a slightly iterative nature to the Estimate (Figure 12.5). Each stage to some extent involves the

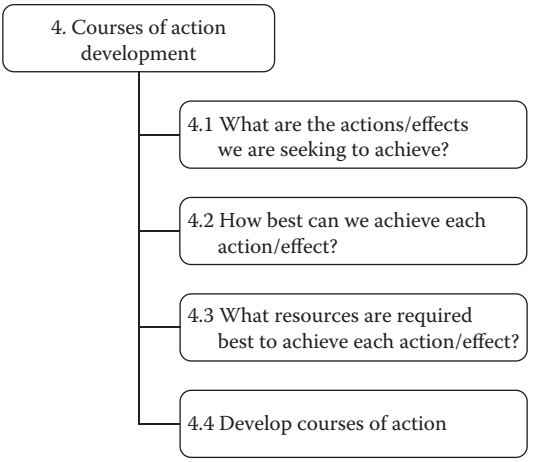

Figure 12.5 Courses of action development.

incorporation of knowledge gained to date. This is particularly true in this section, which starts to pull together outcomes (effects) and map these to the available resources. This gives immediate outputs (what can be done now) and an action plan for closing gaps (what investment is required).

What Are the Actions/Effects We Are Seeking to Achieve?

This is a natural extension of the IRs and overall mission, as identified at the start of this process. This stage may be as simple as just reiterating the IRs, or it may include further refinement based on the subsequent findings. If not done previously, IRs should be prioritized at this stage to help guide the effective allocation of resources.

How Best Can We Achieve Each Action/Effect?

This stage involves consideration of the best way to address a specific IR. This is the meat of product definition, e.g., through a routine report, on an alerting basis, as a project, or a combination of all approaches. Indeed, it is often useful to conduct an initial threat assessment to quantify the potential issues and then institute some form of monitoring or reporting against this thereafter.

What Resources Are Required Best to Achieve Each Action/Effect?

Having worked out potential products, you can then break out the time and effort required to deliver. It is worth breaking out time and resources across the intelligence cycle (direction, collection, collation, analysis, dissemination) in order to thoroughly consider all aspects.

Categories to consider under each part of the cycle include people (skill sets required as well as time); technology, to support all activities as well as knowledge management; and allocation of resources to different IRs. This is also a good point to consider facilities and other infrastructure requirements.

- The output from this is the *management matrix*, which allocates resources to tasks under the headings and in the areas identified previously.

Develop Courses of Action

It is good to consider several courses of action, where possible. This helps to consider things from every angle. If nothing else, there will always be more to do than there are resources available, so some plans can consider what would happen with different levels of additional investment or outsourcing.

CONTROL MEASURES

Having worked out what it is that the intelligence function should deliver, it is then important to consider the architecture that will surround and enable this (Figure 12.6). Some of these are constraints, but many others are factors that will help things run as smoothly as possible. As discussed at several points in this book, this is the heart of effective intelligence management in an effort to achieve the best possible effects from limited time, knowledge, and resources.

What Are the Touch Points with Other Processes?

This entails working out where the intelligence processes can effectively interact with existing architecture and systems. An example would be

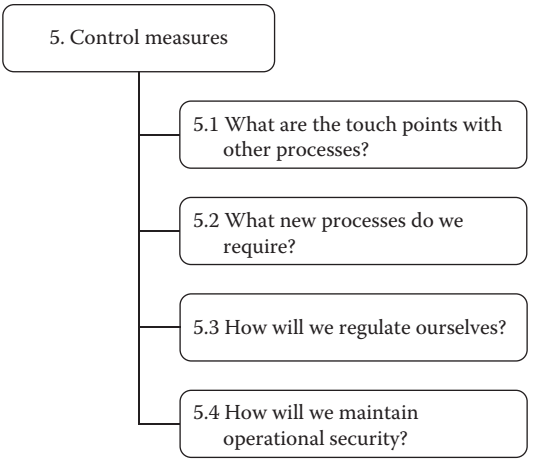

Figure 12.6 Control measures.

presenting intelligence product at routine meetings, risk committees, etc. It could also include integrating with existing systems for measuring ROI or other forms of quality and effectiveness control.

What New Processes Do We Require?

This is fairly self-explanatory: What is required that is missing? This is likely to continue for all parts of the intelligence cycle. SIDeARM, or another model, can be used to help work out processes, although these will always be specific to the organization (and depend upon the size, approach, and resourcing available for the task at hand). One of the most important aspects to consider here are the potential SOPs; see the comparatively exhaustive list in Chapter 6 for more on these.

How Will We Regulate Ourselves?

This covers the confirmation of policies on legal issues, data handling, ethics, and standards of work.

How Will We Maintain Operational Security?

This is broken out due to importance; as previously discussed, it can be critical to success. Areas to consider include IT, data, communications policies, and access control.

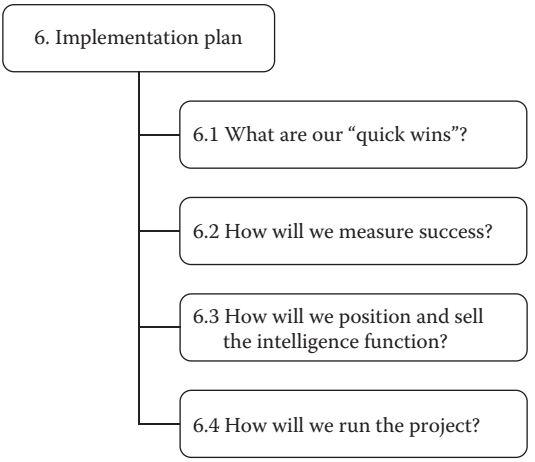

Figure 12.7 Implementation plan.

IMPLEMENTATION PLAN

The implementation plan (Figure 12.7) is the final stage, incorporating all of the previous information into a firm, fully fledged plan to support the implementation of the function. This can also act as the business case, if required.

What Are Our "Quick Wins"?

The aim here is to commence an effective output and start "revving up" the system. As previously discussed, success helps fuel further demand and additional resources, so it is important to get going with at least some sort of product. In most organizations there will be at least some form of intelligence work ongoing without recognition anyway, so at least incorporating this into a more efficient structure should bring a quick benefit.

How Will We Measure Success?

Methods of estimating ROI were discussed in Chapter 6. A model should be developed, either purely internally or with input from senior management. Of course setting this up is a double-edged sword, since you will be held to the suggested targets. Therefore, set them with care!

Key performance indicators (KPIs) are in use in many businesses and thus provide a natural way to monitor progress and effectiveness.

How Do We Position and Sell the Intelligence Function?

This is, technically speaking, the business case. However, this is also an opportunity to build out a "sales list" of potential clients and sponsors to engage with. This can be related to the order in which you develop products; if the two things work in parallel, then there will be natural benefits. Again, having a well-considered plan will allow you to introduce the right product, at the right time, for the right person in such a way that you will show progress while avoiding becoming overcommitted (an easy trap for the unwary).

How Will We Run the Project?

This is an opportunity to finally pull together all aspects into a firm project plan. This should include a summary of the aim and objectives, a timeline, and projected resourcing, deliverables, and milestones. Any recognized project approach can and should be used, as appropriate for the organization. A *Gant chart* is a useful way to present all this information in a comparatively simple and easy-to-understand fashion, but this is not essential.

CONCLUSION

This may seem like a long process. It is fairly exhaustive, for sure. However, it is important to consider things in the round in order to pull together an efficient output. Moreover, the maxim that prior planning and preparation prevents a certain form of poor performance holds particularly true in intelligence work. Since practitioners relatively rarely have the luxury of time, it's important to make the most of it when it is available!

Of course, planning is not just for the time when you're getting started. The outcome-driven/effects-based approach is particularly useful in terms of delivering meaningful products at any stage, and the total approach outlined here can be applied in microcosm to any discrete intelligence task.

Ultimately, the biggest failing in most corporate security departments with regard to intelligence is a failure to adequately work out what they

are trying to do and how best to resource that. This can result in the analytical capability being alternately over- or under-utilized, being pulled in different directions, or being heavily engaged in nugatory tasks to little benefit. Soon, products are being sent out just because they always have been, and without real consideration being given to users. At these points, it is even more important to stop and take stock (I suggest at least annually). As a final thought, it may therefore also be useful to consider using the approach outlined here as a form of "intelligence audit" to confirm that things are still on track. This can tie in with a client feedback process and other forms of review. This also provides a great opportunity to make sure that all processes are running as effectively as possible, and to verify that the system is fully tuned up—a sort of health check, if nothing else. This helps guard against complacency, deteriorating rigor, and all the other malaises that otherwise can all too readily set in.

13

Corporate Security Intelligence Use Cases and Examples

CHAPTER OBJECTIVES

1. To explain various use cases and real-life examples of where intelligence has been used to support corporate operations.
2. To impart basic tools, techniques, and procedures for providing intelligence support around specific projects.
3. To show how the previous theory applies to these practical examples.

INTRODUCTION

The background and theory in this book have hopefully set the scene for the most important part of all—the implementation of intelligence to create practical and useful products. This final chapter therefore outlines many real-life examples of where intelligence products can be used to support corporate operations and the different fields in which such support can be offered.

It is, of course, not exhaustive. Ultimately, intelligence is a tool to help quantify/qualify and solve problems for management; hence intelligence requirements (IRs) are best posed as questions to be answered. As such,

intelligence products can—and should—vary widely in order best to address the needs of the end clients (and the organization as a whole). In fact, if products all looked the same, then there would be little point in having a tailored function.

That said, there are common areas of interest for companies. The examples that follow therefore address the main security operating areas of interest, based on the author's experience. These are as follows:

- Travel security
- New market entry
- Scenario planning
- Depth due diligence
- Power mapping
- Routine country and geopolitical risk analysis
- Executive and event protection
- Exercises and "red teaming"
- Crisis support
- Threat and reputational monitoring

To this can be added monitoring of particular issues such as single-issue violence and political activism (SIVPA) or cyber threats. However, these are similar enough to the examples here to not require separate assessment (the approach and techniques are of course exactly the same). Covering all of these is certainly more than enough to keep the average corporate intelligence team busy!

TRAVEL SECURITY

As explained in Chapter 3, the successful prosecutions of companies over intelligence/threat awareness have been related to the security of travelers. Unsurprisingly, this is a major corporate security function, and companies such as Control Risks Group, International SOS (Claus 2009, 2010), iJet, and The ANVIL Group (to name just a few) supply the vast majority of larger companies with employee-travel-monitoring solutions. A major component of these consists of assessing where travelers are and alerting both them and the company's security team of any potential security threats. A sample alert—taken from The ANVIL Group's Travel Risk Intelligence Service (TRIS)—is reproduced in Figure 13.1).

The importance of travel security has been emphasized by a number of recent incidents. The Mumbai raid of November 26, 2008, served as a

Figure 13.1 Example of a travel risk alert. (Courtesy of The ANVIL Group Ltd.)

particular example to many companies, due to the scale and impact on business travelers, who had not previously been directly targeted in India. Many companies scrambled to confirm who was traveling and whether their executives were staying in the hotels affected by the attacks. For some, this was not an easy task. The security team of one major bank was relieved to find that their sole known traveler was safe, despite staying at one of the hotels occupied by the terrorists, since he was out to dinner when the attack commenced and had received word via the travel alerting system. However, they were then very surprised when they got a call from the bank's Mumbai office—as that was the first that they knew of its existence. This may sound incompetent, but the team involved certainly did not fit that description. Rather, it turned out that this office was the product of a recent acquisition that had not yet properly percolated through the organization. This is a salient lesson in how any security function—and, by extension, the intelligence function—in larger, networked businesses

needs to spend significant time on understanding what their employer is doing, and where, in order to ensure that they can provide adequate cover.

A more recent example came after the Tohoku earthquake of March 11, 2011. This quake and the accompanying tsunami killed at least 16,000 people and caused massive infrastructural damage, including three nuclear meltdowns and damage to over a million buildings. In fact, it was so serious that it also moved Honshu (Japan's main island) several feet closer to the United States, and even shifted the Earth's rotational axis. The issue highlighted by the quake, though, was that many companies did not consider Japan a risky location, and so did not track their travelers there due to the low assessed threat level. This again left many scrambling to find their people—reinforcing a lesson learned less than a month before, albeit in a more minor way, by the earthquake in Christchurch, New Zealand, on 22 February.

Intelligence would not necessarily have predicted these natural disasters, although a clear understanding of threats in both countries would almost certainly have indicated that these were possible hazards, and that increasing population pressure is driving more and more development in areas vulnerable to destructive threats of this kind. (On which note, it may also be worth mentioning that Istanbul lies on the Anatolian Fault and on current trends is well overdue a highly damaging earthquake.) To be honest, before the Japanese disaster, if someone had suggested an exercise scenario whereby a first-world country suffered a severe tremor, tidal wave, and then nuclear meltdown, it would probably have been regarded as a laughably worst-case scenario that was not realistic. Let that be a lesson.

The key point is that tracking and alerting of travelers is important. However, this is essentially reactive. Knowing that an incident is happening is of course useful—witness our banker friend who was fortuitously out to dinner when terrorists attacked, and was warned not to go back to anywhere near the hotel. However, how much better to know that an incident is about to occur. This is also a critical enabler, going back to the fact that intelligence should be helping to make money for the organization. Thoroughly understanding a situation—and being able to predict, with some degree of accuracy when risk factors may be going to occur—is a critical *enabler* of business. To go back to the India example, after the Mumbai attacks, many major companies blindly applied travel bans. These applied not just to the city, but to the entire country. In some cases, these bans lasted for months, even for companies that had Indian offices. The financial impact on business must have been enormous, and ultimately

the blanket bans proved to be completely senseless. Organizations with a more refined understanding of the situation were able to continue their operations with much less impact, also winning them valuable praise from the Indians in the process, who resented the companies that had, in essence, run away. That is not to say that risks did not remain, but there were clear *triggers*, *indicators*, and *warnings* that corporate intelligence teams were using to measure the risks of further travel security threats emerging.

A significant role for intelligence teams is sometimes working out whether to allow travel—or, rather, under what conditions to allow travel—when a situation is emerging. A recent example is the crisis over Syria following the August 21, 2013, chemical attacks outside Damascus. Obviously, few organizations had many people inside Syria, – the exceptions being NGOs and media companies. However, many had people in Lebanon, Israel, and Jordan, and concerns were also raised about the safety of travelers in the Arabian Gulf. Obviously, fine understanding of the nuances of the situation was required in order to work out the best options. A blanket ban on travel would be costly, and so developing an enabling policy would offer real decision advantage. Soon after the reports of the incident emerged, intelligence teams were therefore considering:

- The possible international responses to the chemical incident
- The timeline for potential actions
- Which nations might be involved
- What the response of Syria and its allies would be to possible actions by the United States and its allies
- Where these responses could take place
- What other actors may seek to take advantage of the situation
- What the second-order consequences might be of the various possible courses of action ahead, e.g., over the oil price and so on

As you can see, this is a spread of activity from the tactical to the strategic levels, and this understanding goes way beyond just providing travel advice. During these crises there is a high degree of appetite for intelligence, so this is a great opportunity to put the capability in the "shop window" by making the security intelligence team's insight available across the organization. In this case, more detailed outputs could include:

- Travel advice enabling business to continue in the region, with emphasis on where extra caution might be required (Lebanon being the country most affected early in the crisis)

- Understanding of how and where else threats could emerge in response to a US-led strike—for example by Lebanese Hezbollah or other Iranian proxies striking against targets in parts of the world where they have capability, or from the Syrian Electronic Army in cyberspace
- Development of measures to help the business reduce its vulnerability to potential threats—supporting activities to prevent, protect, and prepare (including creating "most likely" plans for exercises)
- Definition of scenarios to enable business strategic decision making
- Understanding of medium- and long-term consequences, e.g., raised oil prices for a protracted period (of potential benefit to doing business in countries such as Russia and Azerbaijan)

Of course throughout all this, the team also had to avoid being sucked into doing so much on this one situation that they missed other things going on. For example, at the same time as the Syria incident emerged, Libya began to show signs of increasing destabilization, and Egypt saw jihadist attacks spreading to the Suez Canal and even to Cairo—both of interest to corporations. Meanwhile, mass protests in Latin America saw attacks on corporate interests in Brazil and the protracted closure of airports and government buildings in Mexico. Just because there's a crisis in one place, life doesn't stop everywhere else! Given that the main feature of a corporate intelligence team is, in effect, to guard against surprises (low-probability/high-impact scenarios), at these times it's even more important to look beyond the obvious.

NEW MARKET ENTRY

Intelligence departments often show their worth when a company enters a new market. As discussed in the first few chapters of Section 1, the trends of trade and globalization, coupled with geopolitical and climatic developments, are driving companies to do more and more business in areas of heightened security risk. Quantifying this is therefore an increasingly common task. Again, this is a great activity to be involved in, as it helps the organization to operate effectively, with security being seen as an enabler, as long as the tone is correct.

Companies are, of course, particularly well set up to carry out market analysis, assess economic and financial risks, and decide on business cases. This is because they tend to understand their core operating environment very well. Indeed, they wouldn't survive, otherwise. (Incidentally, many

of the principles of intelligence are used in, for example, competitor and market analysis; it is just that they are often buried under the mechanisms that are applied for these sorts of commercial enterprises.) However, the security environment remains much less understood, and this can be a critical aspect when establishing a new venture or when deciding whether to proceed with a project or investment.

Approaching analysis of the risks around a new market is, of course, a daunting task. One of the standard approaches is known as PESTLE analysis. This stands for

- Politics
- Economics
- Sociology
- Technology
- Legal
- Environmental

Note that variations of this technique exist. You may also see PEST referred to, or STEEPLED, although these all mean more or less the same thing. In STEEPLED, the D stands for demographics, although it is usually simpler and more common to put this under *sociology*.

As an example of this in use, a particular client was looking at which of two African countries it was going to expand into. They understood the respective markets to a very detailed level but had no mechanism for the board to understand the wider situation in both countries and thereby make a decision; security was a particular consideration. Without a template, coming up with a thorough assessment in the time available would have been very difficult. What greatly helped was the development by the author's team of a standard series of questions for addressing new market entry. These are presented in Table 13.1.

The aim is not to be able to answer all questions straight off the bat, as that would be highly unusual. Instead, the goal is to provide what is in effect an off-the-shelf list of *intelligence requirements* (IRs). This is why the points are all shaped as questions. The process of finding the answers serves as a guide to the analysis and ensures that all possible angles are covered. For this particular client, we maintained a spreadsheet with all these answers, which served as a form of work plan to pull together effort and insight from across the business. Of course, getting some answers may be hard or require further iterations of work. Therefore, it's best to regard the template as, in effect, a master plan, and the resulting body of knowledge should be continuously developed and added to when working on this sort of project.

Table 13.1 Tailored estimate: Questions for addressing new market entry

Task Analysis

What are we trying to do?
- Specified tasks
- Implied tasks

Why are we doing it?
What are the critical success factors?
What is the timeline?
What other constraints are there?

Consideration of Factors

Political

- What is the political/power structure?
  - Legislative/executive framework
  - Parties and policies
  - Key personalities
  - Geographic overlay of support
  - Nongovernment actors
    - Trade unions
    - Religious groups
    - Tribal alliances
- What are the external factors affecting the system?
  - Neighbors
  - World bodies
  - Great powers
  - NGOs
  - Transnational issues
- What are the key political dates to watch?
- What are the scenarios around these decision points?

Economic

- What is the general economic trend?
  - Macro
  - Micro
- What are the critical economic assets/dependencies?
- What are the forecasts for:
  - Disposable income
  - Employment

Table 13.1 (*Continued*) Questions for addressing new market entry

- Financial Exchange
- Interest rates
- Inflation
- Foreign investment (including trade policies)
- Taxation
- Cost of basic goods
  - Fuels
  - Milk
  - Staples
- Housing

How might these factors change following political flashpoints?
What are the key influencers around financial crime?

Sociological

What are the most important demographic factors?
Is there any significant tribal/ethnic breakdown or culture that may impact operations?
How might lifestyle issues affect operations?
What is the education level?
What are the key aspects around public health?
What is the religious landscape?
How will values and cultural mores affect our business?

- Staff attitudes
- Customer attitudes
- Market attitudes
- Organizational culture

What are the most likely future shifts and drivers for change?

Technological

What is the current level of technological development, adoption, and capability?
What is the communications infrastructure like?
What is the speed of change and what effects will this have?
What is the IT literacy?
What is the cyber security landscape?

- Threat actors
- Protection measures

Continued

Table 13.1 (*Continued*) Questions for addressing new market entry

Legal
Ethics
Current situation
Future situation
Transnational legislation
Regulatory bodies/processes
Employment law
Company law
Consumer protection
Competition law
Environmental
What are the key security aspects?
International
Insurgency
Terrorism
Activism
Crime
Travel security
What is the state of transport?
Climate: effect on operations?
What medical/health aspects are there?
What other natural hazards exist?
Evaluation/Scenario Planning
System/concept maps
Best case
Worst case
Median/most likely case
Key decision points/areas of interest
Identification of depth intelligence requirements

Source: © Sibylline Ltd., 2014.

SCENARIO PLANNING

Scenario planning is a key skill for intelligence teams (Figure 13.2). Although now common as a strategic planning tool in corporate life, it was initially developed by military intelligence, so it's fitting that this has come full circle. In geopolitical terms, this was closely linked to game

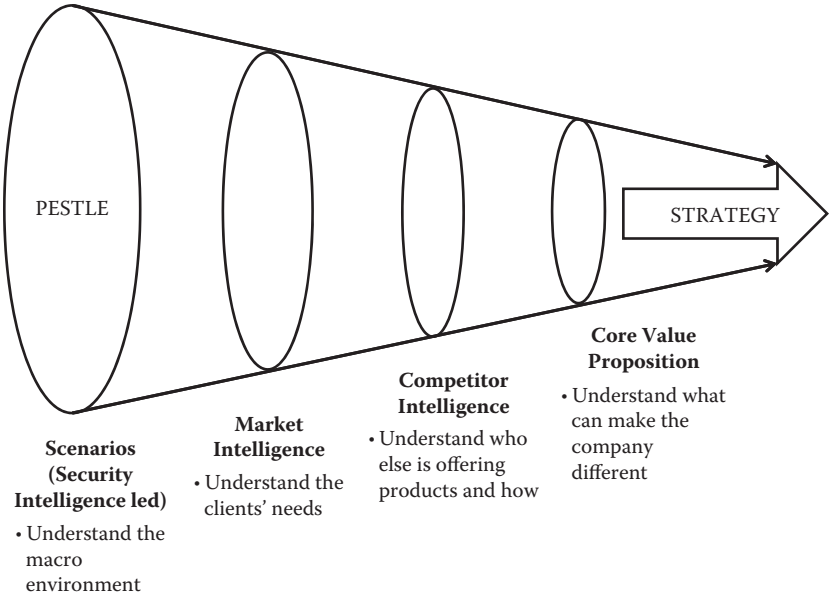

Figure 13.2 Intelligence-led scenario planning and corporate strategy.

theory, whereby opponents were modeled and possible action/reaction cycles were modeled and analyzed. However, in the corporate environment, the threat angle is usually outside the control of the company, so the task is more about understanding the best course of action through a series of possible events. This therefore differs from traditional *contingency planning*, which focuses only on one particular situation or uncertainty, and which rarely involves essentially testing a situation to destruction (starting at the worst possible case, in other words, and remember the Tohoku earthquake as an example of how this can actually come to pass).

A good example that was studied by many companies was the possibility of a US or Israeli strike on Iranian nuclear facilities in late 2012. This would be a significant event, with consequences that would not be well understood and could be particularly unexpected. Scenario planning offered an effective way to work through and understand the situation with reference to what was known, what could be surmised, what was possible, and what would be critical to the particular company undertaking the planning exercise. This experience could be used to help deploy mitigation measures, including internal business-continuity exercises.

Note that effective scenario planning often involves the systems approach, discussed in more detail later in this chapter. This is because events never happen in isolation; rather, they always have second- and third-order consequences. These are usually much less obvious, and it is these factors that can catch organizations by surprise, so this is a critical angle throughout most intelligence work. Indeed, analysts sometimes feel like they have to think three moves ahead for each potential issue or scenario they may be considering. This is why sharing the experience of scenario planning can be so effective, because many different bases of experience, knowledge, judgment, and observation can be brought to bear. Moreover, the shared experience of working through scenarios helps acclimatize managers and decision makers to the fact that uncertainty is pervasive, and there are often multiple futures to be considered. Understanding the drivers and the likely range of outcomes allows for resilient and adaptive responses, and for sensible and well-informed decision making, especially by comparison with betting on one outcome. Moreover, doing this in a relaxed and controlled environment ahead of time, rather than when in the midst of a crisis, is clearly a major advantage.

Based on the military approach, the key steps in scenario planning are as follows:

1. *Scoping*: Define the question, topic or issue you want to address, and work out the parameters and limitations in terms of time or geography.
2. *Stakeholder analysis*: Consider personalities of stakeholders and their track records.
3. *Trend analysis*: Identify the external forces in operation, and clarify how these act.
4. *Modeling*: Develop linkages and identify nodes, decision points, and outcomes. Where possible, find quantitative information that can drive the assessments.
5. *Scenario development*: Allocate probabilities. Use an iterative approach to converge on certain varied, yet plausible, scenarios.
6. *Business mapping*: Overlay business operations onto the modeled scenarios (this is where this stops being a purely intelligence-team focus). For security purposes, seek to identify the worst-case scenario and spot any "spikes" in terms of exposure.
7. *Action planning*: Identify early-warning factors, key trends, and indicators. Seek to mitigate against the "spikes" in exposure, as this usually

offers the greatest cost benefits. In the security function, the outputs should inform the prevent, protect, and prepare work strands.

8. *Monitoring*: Monitor and assess the model and scenarios, and detect any changes or hardening in the scenarios being planned.

Of course, by now it has probably become apparent to you that scenario planning is just the first stage in handling the future effectively. As Paul Schoemaker (2012) states in *Profiting from Uncertainty*, the real work is then crafting flexible strategies and, from the intelligence point of view, effective and appropriate monitoring systems. Shell, which along with General Electric was one of the first companies to really use scenario planning (especially following the oil shocks of 1973), found that the lasting benefit of the process was actually undermined not by the intellectual rigor of the scenarios and multiple futures considered, but rather by the

SCENARIO PLANNING: FOR ACTION OR JUST PREPARATION?

The finding that managers do not make the most of scenario planning is reinforced by Arie de Geus (1992), formerly group planning coordinator for Shell, in an article titled "Modelling To Predict or Learn." He points out that managers in the company were rarely willing to act on the information because they did not have confidence in the predictions, even though these were largely right and offered Shell an important decision advantage, had they been acted on. De Geus summarizes this as being due to decision makers wanting to make up their own minds, and only trusting their own judgment, due to the fact that ultimately they carry the responsibility. He links the fact that many senior executives are clever people, and so they clearly understand the penalties for failure, which makes them hesitant, and learn "less and slower" than they would have done otherwise. His view, then, is that scenario modeling offers the real advantage of allowing decision makers to "play through" their options in a simulated environment, even if this is only in their heads, when reading the report. This helps them learn and shape their perceptions so that they can better make sense of events as things mature. This is an important facet to bear in mind when preparing intelligence material: Take the reader on the journey and present the facts in such a way that they can "make up their own minds."

subsequent decision-making processes that did not use the knowledge and wisdom gained. However, the reasons for this may now be changing, with increasing access to information and improved abilities to process and model risk outcomes increasing managerial confidence in the accuracy of scenarios and their applicability to "the real world."

DEPTH DUE DILIGENCE

The term *due diligence* appears to first have been used in the US Securities Act of 1933, where it referred to the obligation of share brokers to conduct adequate investigations of companies whose stock they were selling. It remains an investigative and assurance activity most strongly linked to the financial sector, but is expanding much more widely, especially since the adoption of the Foreign Corrupt Practices Act (FCPA, discussed in Chapter 2). This mandates both *initial* and *ongoing* due diligence for relationships where corruption could possibly be a factor, principally meaning emerging markets. Meanwhile, the wider need to prevent fraud, obey relevant sanctions, and safeguard investments also requires at least some form of due diligence (and this is often mandated by regulators).

Although much transactional due-diligence work is the responsibility of the legal/compliance departments, security departments are becoming ever more involved in three main areas:

- Screening
- Enhanced due diligence
- Investigative due diligence

Screening

As discussed previously, some legislative requirements require organizations to screen agents, counterparties, and clients for countering corruption, terrorism, international sanctions breaches, and crime. This is usually a basic function, but where larger-scale requirements exist, this can be done effectively in-house by an intelligence team. The process is usually automated, with a degree of human oversight. Both open-source and human-source information is used to come up with assessments, with analysis of social media being a growing trend, and facility in foreign

languages being highly desirable. Databases are often outsourced and can be checked on a subscription or pay-per-view basis.

The aim of the screening process is usually to search large amounts of information for red flags, meaning that a particular person, account, or transaction will require further investigation. This is why technology is usually such an important part of the solution, and name-checking software is available free or at low cost on the Internet. This, coupled to feeds from databases (to which other parts of the enterprise may already subscribe), forms a key enabler for managing this task effectively.

Enhanced Due Diligence

This tends to be more of a requirement in higher-risk markets and is effectively mandated by anti-money-laundering regulations, know your client (KYC) codes, and counter-corruption legislation such as the FCPA. Enhanced due diligence usually covers investigation into business partners/clients where particular risk factors have already been deemed to exist, perhaps just because of the location of the deal, but also possibly as a result of factors identified during basic screening. The aim is to conduct as full an assessment as possible of the risk factors around a particular relationship or project. Again, the level of diligence is basically dictated by corporate responsibility and how much risk the organization is willing to tolerate. A basic test would be that the organization has thoroughly undertaken efforts to find out as much as is reasonably possible about the entity and the individual they are doing business with.

Many organizations view enhanced due diligence as having two tiers. Tier one is generally in-depth open source, public record, and database searches, used to verify facts and see any obvious red flags (causes for concern). Tier two, always applied in higher-risk countries where records may not readily be available, is to conduct local searches and checks using on-the-ground sources. There is a thriving industry in conducting these checks, and of course it is usually impractical for even the largest organizations to attempt to do this themselves, not least because of the vast range of language skills required. Some or all of the function is therefore usually outsourced.

Fully outsourcing this function makes sense for smaller businesses, where the requirement is an exception rather than a rule. However, for companies where higher transaction volumes are expected, the best practice is to have an in-house analytical capability with access to the databases that fuel tier-one searches. The analysts should have the languages of most

interest to the organization. Although this is a significant investment, the ability to focus external resources only on matters of the most concern offers a major advantage in terms of cost efficiency. This also helps ensure that information on the company's customers or transactions is not constantly being fed outside the organization—a potential point of vulnerability.

As enhanced due diligence tends to be related to transactions, there is often an emphasis on timeliness. This requires highly efficient processes and reliable access to sources. Moreover, the requirement should be enshrined somewhere into the organization's procedures, for example as part of a compliance workflow. The reason for this is simple: Although it is a crucial activity for the organization to undertake (from legal, regulatory, financial, and ethical standpoints), the reality is that people in sales-type/client-facing roles will inevitably see this as an impediment rather than an enabler. After all, no one likes to be told that they can't do business, especially when they are incentivized by performance-related bonuses. Moreover, sales teams can be from the same geographic area as the subject of the due diligence process, which means that their risk appetite may be different from those of the organization at a central level. In these circumstances, it is vital for there to be some form of "top cover." This also applies to funding, since normal practice is to bill back the costs of an investigation to the business unit that has required the work, which can add to resentment. Imagine not only not being prevented from doing a piece of business, but having to pay a substantial amount to be given that advice! This is a barrier to undertaking due diligence, which is a problem for the company as a whole. Therefore, one of the best approaches that we have seen is for the company (a bank, specifically, in this case) centrally to pick up the tab for the work, centralizing the function within the security department. This is coupled with the enhanced due-diligence process being clearly worked into the company's procedures, and all involved being clearly educated on the need for such work in order to stave off serious reputational and financial issues. This has resulted in much lower barriers to cooperation from client-facing teams, and so should be considered the pinnacle of best practice when considering implementing enhanced due diligence.

Investigative Due Diligence

The term *investigative due diligence* is used here to cover the range of activities where due diligence is required due to circumstances. An example might be where a company receives an anonymous warning of wrongdoing in

a partner organization or by a client, which happens more often than one might think. By some measures, support to new market entry would also come under this broad heading, since that tends to involve an analysis of risk factors around a particular partner, client, or opportunity. Again, much of this activity is to some extent voluntary, being dictated by the company's level of responsibility and risk appetite.

Because it is often nontransactional, investigative due diligence tends to be a slower process than enhanced due diligence, which is often laid down as part of an internal process (as discussed previously). Some investigations have taken years, in effect becoming standing tasks for the intelligence function. Due to the broad range of potential subjects and circumstances covered, it is hard to give absolute guidance. This has formed the topic for many books in and of itself. However, adopting the basic intelligence approaches outlined in Section 2 will stand any practitioner in good stead, particularly in regard to target-centric analysis.

POWER MAPPING

Power mapping is a capability that follows naturally from the tools, techniques, and procedures of depth due diligence. As described previously, this is of use to businesses, as it helps identify a target individual, e.g., someone the organization may want to influence for policy or commercial reasons. Although often conducted as a single project, this is perhaps best conducted as a rolling task in support of a business division or to aid the development of opportunities in a defined geographical area (e.g., mapping out power relationships in an Arabian Gulf state, as discussed in the last chapter). The author has seen this used in intelligence agencies to understand complex relationships, especially within foreign governments—even friendly ones. Power mapping is also popular with activist groups and lobbyists. Indeed, it can be used in any situation where understanding of influence relationships is sought.

As suggested by the name, power mapping is largely a visual process. Laying out the relationships provides an excellent reference and supports the evolutionary approach of the task, whereby knowledge is gradually added to the diagram. Technology can help automate the development of the network. Many of the same methods therefore also apply to investigations, especially when trying to make sense of complex relationships, and also to target-centric network analysis—discussed in the next section of this book.

There are various approaches, but the following are the general stages to effective power mapping as an intelligence activity:

1. *Determine your target*: Place the target that you are seeking to reach, or the objective that you are seeking to achieve, at the center of the map.
2. *Determine your scope*: As discussed previously, this approach works best within well-defined parameters.
3. *Map your target*: Research the target and find first-order connections to people, places, and organizations.
4. *Map people who have suspected links to or influence over the target*: Research each entity and expand on the detail available. Draw relational power lines to show connections.
5. *Map "friendlies"*: Place known personalities or organizations on the diagram. This could include, for example, existing clients or advisors. Again, then define relational power lines.
6. *Identify knowledge gaps*: Hopefully, if you set the scope correctly in stage 2, some connections should already be evident. This gives you an immediate route to the target you wish to influence or understand. However, if not, then at least the diagram may suggest the start of a course of action. Adopting an iterative approach, searching connections for every known contact, will over time suggest a path to reach the target.
7. *Identify priority relationships*: The power map will show people who have the most connections (or the most important ones), and who are therefore "key influencers" or "nodes" in the network. This makes them more valuable, and they can be passed to operators for action.

Although seemingly simple, this approach can take a great deal of time. Researching each target tends to require use of open sources, databases, and human sources to flesh out the picture. Moreover, a power map is an ongoing piece of work—it will never be fully complete or 100% up to date. However, the visual tool is a very effective aid to understanding, and it is extremely useful for communicating insight to decision makers.

The time taken to understand these networks to some extent mitigates against using advanced data-mining tools or intelligence software. In the author's experience, these never tend to work well, instead generating either obvious or meaningless connections that are not thoroughly thought through, and take as long to clean up as they would have done to have been built from first principles. (The exception is where large

amounts of structured data need to be compared.) Others are frankly overpriced, being intended to exploit the deep pockets of the government buyer. The most favored tool is therefore a basic, readily available drawing program like Microsoft Visio or the many freeware equivalents. These allow for entities—simple text boxes—to be linked and moved around without losing the connections between them. These connections can themselves be labeled. Shapes, colors, and weight of lines can also be used to indicate the nature and strength of relationships.

Note, however, that this approach works best for projects where finding the data takes longer than recording it and building the connections, as is typically the case when undertaking traditional power mapping. In contrast, sometimes investigations require spotting connections in huge amounts of data, for example phone records. In these cases, technological solutions generally come to the fore in order to make sense of the vast array of data. (Although it is surprising what can be done simply with Microsoft Excel and other ubiquitous programs, and careful thought trumps technology alone every time!)

COUNTRY/GEOPOLITICAL RISK ANALYSIS

A variation of terms can cause confusion when considering this area. At the strategic level, the terms *country risk* and *political risk* are often used interchangeably, but there is little agreement on what these phrases mean. Country risk often tends to be used in financial contexts, with a focus on economics, while political risk is perhaps a term in more general use, and that is gaining in currency. We tend to prefer the term country risk, as in a security context we feel that this better captures the range of activities undertaken.

Ongoing country-risk analysis overlaps hugely with new-market-entry analysis, travel security/monitoring, and scenario planning. The aim is to protect travelers, assets, relationships, supply chains, or investments by understanding current and emerging risks. In general, country-risk work should therefore be related to security processes, for example restrictions on travel or limitations on hosting large events in the country of concern.

Country-risk analysis can have benefits extending far beyond security. For example, many banks use the security department's analysis—whether in-house or outsourced—to help justify the risk levels they have assigned to investments when talking to the regulator. As discussed in previous chapters, this can be a source of significant profit for the organization.

There are two real factors to this work: understanding what is happening now, and predicting what is likely to happen in the future. As with much of intelligence work, the main effort is understanding low-probability/high-impact scenarios or, in simpler terms, anticipating surprises. This helps prepare the organization and enables appropriate deployment of mitigation should such events come to pass. Much effort is therefore spent on identifying triggers, indicators, and warnings.

The art and science of country-risk analysis is worthy of a book of its own; indeed, many have been written. However, the principles of intelligence discussed throughout this book apply here as anywhere else, and it is important not to get too sucked into the weeds when considering, for example, the finer points of economics. Often, in organizations, there are whole departments focused on markets and finance. In contrast, the role of the security intelligence function is to put all the available information into clearer terms—answering the key question: "What does this all mean for the resilience of the organization?"

Covering the geographical spread of a large organization is nearly impossible for a small intelligence team, which could not possibly have the time and resources (especially languages) to deal with discovering the implications of events globally. Instead, normal practice is to use vendors to provide this sort of reporting, and then for the in-house analysts to draw on this pool of knowledge when creating internal assessments. Obviously, where funds allow, it is best to use a range of vendors in order to gain several points of view—plus some will inevitably be better than others in certain aspects.

Horizon-scanning for emerging threats is also a key aspect of work in this area. Again, the role of the in-house analyst is often to spot emerging possible incidents that are of the most relevance to their particular organization. On occasion, this may also entail filling in the blanks left by others' analysis. As a vendor myself, I have often gained what I term "second-order insight" while talking to clients, as they have had the luxury of considering the refined intelligence produced, rather than having been caught up in the mechanism of actually divining the meaning in the first place! This is a reminder of how intelligence really can be an iterative process, and why outsourcing can be such a benefit in this particular area.

If actually conducting the work, there are two main models for reporting on country risk. One is to discuss themes and events as they break. This ensures maximum interest in what is being produced. However, this is not particularly predictive; by only reporting when things are happening, you often miss the opportunity to highlight them in advance, enabling

preventive action to be taken. In contrast, periodic analysis—whereby risk factors are reviewed and trends analyzed on a regular basis—enables a better "forward looking" approach to be taken. After all, the real value of analysis comes from making links that may not be obvious; again, low-probability but high-impact scenarios are of the most importance.

PESTLE may be used as a guide of what to consider in country-risk analysis, although other techniques exist. A good approach is always to conduct an initial country-risk assessment to identify key themes, triggers, indicators, warnings, and risk outcomes (scenarios). This can be kept updated as a "rolling brief" for those getting to know the country for the first time (for example senior executives visiting or being posted there); this report also sets out the organization's view of what is important in regard to the country, providing a baseline for decision making.

These rolling briefs should be kept updated by more "current" intelligence, in the form of periodic reports. The periodicity can vary in accordance with the intensity of the operating environment; two weeks usually seems right for most countries, although a situation like that in Iraq might reward daily reporting (although trends would still emerge over longer periods of time). Periodic reports to examine strategic/operational trends should be supplemented by analytical reports when situations break, and occasional in-depth briefs on specific issues, in order to provide a detailed picture of the country under observation.

A question that always emerges is whether quantitative or qualitative analysis is more important. Ideally, country-risk analysis (for security/political ends) should contain both. The issue with numbers is often that any model is inherently imperfect, primarily due to the lack of completely clear information regarding the sort of complex system represented by a country. Many analysts therefore find that the results generated don't match their qualitative assessment or "ground truth," and so end up tweaking the numbers anyway in order to provide the "right" level. This is, perhaps, no bad thing, as in essence it combines both approaches. Related to this, a common approach for in-house teams that have outsourced their background country-risk work is to normalize the opinions of several providers and use this to fuel their internal processes. Ultimately, though, the highest value is often represented by the analyst's gut feel and, again, interpretation of what is most relevant to the organization. Focusing on this level ensures that the "so what" question is answered, and that second-order consequences are observed well ahead of the rest of the pack.

EXECUTIVE AND EVENT PROTECTION

Intelligence support to executive and event protection usually focuses on a very tight series of intelligence requirements. Reputational monitoring around senior executives is an increasingly common task, especially as more and more personal information is ending up on the Internet, due mainly to the use of social media. This remains a vulnerability for many companies. Even though the executives themselves may be careful with their information (not always the case), family members are often much less so, and it is frankly amazing what can be found out. A classic example in the UK was the case of the new director of the Secret Intelligence Service (SIS), whose wife's Facebook profile was not restricted. The media rapidly found this out, and the world was treated to views of him in his swimming gear—surely a first for a service whose very existence was denied less than twenty years ago! Another example is family members who visit (e.g., cousins or siblings) and take geo-tagged photographs of executives at home, showing exactly where they live. Although social media streams are now much more sanitized than was once the case (see the chapters on Intelligence Collection and Collation, Chapters 7 and 8, respectively), there is still huge dynamic value to the data that is available, especially when combined with other freely available services. Again, it is perhaps important to remember that all the material and approaches that make enhanced due diligence easier than has hitherto been the case can work against you as well as for you.

A useful exercise (tied to red-teaming; see next section) is to assess what is openly available on senior executives by starting from an attacker's point of view and level of access. For example, take the CEO and see what can be researched about them and what sort of picture builds up. If they are called John Smith, then this may be harder than if they have an unusual name, but regardless, the results will sometimes surprise the board member concerned. A particular European bank did this for their CEO, who played down the findings only to be "jumped" a few days later by a reporter and camera crew who had analyzed his movements. Although damaging material from this ambush ended up on the Internet, it could have been worse; another board member had his house broken into and laptop stolen in a very targeted operation. The assailants in that case would most certainly have gathered as much intelligence as they could have beforehand.

Due to the importance of travel for senior executives, often there is an extra focus on their security; this may even be a legal requirement. In such

cases, an analyst may be asked to conduct a *threat*, *risk*, and *vulnerability assessment* of the trip, as discussed previously.

It is often not appreciated that executive protection is in fact a constant process of risk management and mitigation; a close protection team is always considering exposure and potential "actions on." It is therefore a process very much led by intelligence, at all of the tactical, operational, and strategic levels.

EXERCISES AND "RED-TEAMING"

Exercises are not generally popular with senior decision makers. At its best, an exercise should be a learning experience, and the aim should be to test things to a level greatly above what could be expected in practice—"train hard, fight easy," as the British army puts it. However, this generally means taking people out of their comfort zone, and may expose the senior decision makers to a position where they are seen to "fail," despite this being of great personal and organizational benefit. All too often, exercises are therefore omitted, but this is a trend that should be combated where possible.

The intelligence team has a role to play in this by convincing people of the "most likely" and "most dangerous" scenarios. This can form a valuable part of presenting an exercise, and the "real world" setting helps obtain vital buy-in from participants. If done well, and in an interactive way, exercising against these scenarios can very much help teams react. Working together at least once builds significant confidence across a mixed team (e.g., for a crisis), and really helps to prepare people mentally to deal with challenges. Although they are unlikely to have analyzed the exact situation that occurs, this mental preparation is of great importance. Remember, people in a crisis do not raise to the level of their aspirations; instead, their performance falls to the level of their training and preparation.

Having said that the scenario will rarely play out the same in practice, it is important to recount the tale of one British financial organization. They conducted a security exercise for the crisis team based on the intelligence team's assessment of a likely scenario. Their belief was that an attack on London was imminent, and it would involve multiple suicide IEDs targeting transport in order to cause chaos, confusion, and mass casualties. The exercise taught several valuable lessons about the organization's ability to cope, and drew on previous experience as a

target. Early the following day, the chief security officer received a message about multiple devices detonating across the city. "The exercise was yesterday," he carefully explained, only to find out that he had just received news of the 7/7 bombings. The intelligence team—based on a great assessment and sound work—had got this spot on, despite the UK government recently lowering the threat level. The intelligence-led exercise ultimately allowed the organization to respond smoothly to this serious business-continuity challenge.

Another role for the intelligence team in such exercises—or even as part of more routine assessments—is in *red-teaming*. This is a term reflecting thinking from the enemy ("red") point of view. The red team seeks to consider the organization with the enemy's mindset in order to help spot vulnerabilities and issues that may not immediately be obvious. At the most basic, it is walking the perimeter thinking like a hostile actor. As discussed in Chapter 2, Rick Rescorla did this at the World Trade Center ahead of the 1993 attack, allowing him to spot the physical vulnerability that was eventually exploited by jihadists. Finally, as discussed in Chapter 7 on analysis, being able to present from the enemy point of view makes it easier for some analysts to state their mind, since they have a "license" to challenge established thinking without being seen to confront their day-to-day hierarchy.

CRISIS SUPPORT

Crisis support follows naturally as the result of scenario exercises. Ultimately, the intelligence team's main value is in bringing clarity to what is often a confused situation. This may include putting an unexpected event into context; advising on possible future developments; advising on the effects of possible courses of action; and presenting the business with a common operating picture drawn from various sources, both inside and outside the organization. The chances are that a higher than usual tempo of reporting will be required; the manager may have to reallocate resources at short notice, and it is here that standard operating procedures (SOPs) really come into their own, giving the ability rapidly to retask assets in support of immediate needs. To some extent, the intelligence team must also be able to anticipate the needs of the decision maker and communicate clearly in order to manage expectations (e.g., promising when a report will be made available, and not delaying it in order to make it more comprehensive, a common error). Intelligence should have an

input in crisis meetings or calls, and should generally be the lead item, setting the context for all decision making that follows.

THREAT AND REPUTATIONAL MONITORING

Steady-state monitoring of threat and reputational issues is a highly useful field for corporate intelligence teams to handle. This often consists of an initial threat assessment, which is used to set more specific IRs, followed by periodic reporting supplemented by alerts. Reputational monitoring in particular is of great use to the business, and it is viewed as an activity that is linked to revenue in a much more tangible way than other parts of security. Moreover, it can be approached in exactly the same way as any other intelligence challenge. Extensions of this include, for example, monitoring for pirated or stolen product, or looking for product reviews that show a negative reaction, e.g., for a pharmaceutical company looking to see if there are problems with any of its drugs out on the market. Apple is known to do this on a macro level in order to see if there is an emerging hardware that needs to be addressed. This can be handled alongside more security-related issues, given the clear overlap in collection, especially when considering social media keywords and the like.

SUMMARY

The examples presented in this chapter merely scratch the surface of what can be done in regard to security intelligence. Again, it is ultimately a function that is orientated around helping solve problems through bringing clarity and insight, and so the intelligence approaches outlined here are of use in tackling a whole range of issues. As corporate security becomes ever more a part of the business, so the value of what the intelligence team can bring to bear will become ever more assimilated into the mainstream. Doubtless, the list of tasks will then increase—but such is the price of success!

14

Conclusion: Reinforcing Intelligent Security

I hope this book has shown how corporate security intelligence is a vital function, especially in the modern age. Drivers include the increasing legal and legislative imperative; pressure from society and shareholders; the multiplicity of current and future threats; the trend of globalization, for even the smallest organizations; enhanced scrutiny; and ever-increasing access to information. The latter has enabled a vastly increased reach for intelligence activities of all kinds at little cost, which has also increased the return on investment of establishing a team.

Ultimately, if done well, corporate security intelligence helps to

- Prevent threats from emerging
- Protect the organization appropriately
- Prepare the organization for likely events
- Drive profit!

It does this by driving both savings and benefits, allowing organizations to make better use of limited resources and drive security forward in a more efficient fashion. Ultimately, this results in security being less of a cost to the business and more of a benefit. The insight from the intelligence team can also help drive the highest levels of decision making, helping to position the security function at the top table and established as more of a facilitator and aid to business. Sound intelligence work also helps obtain buy-in for the business when presenting the business case for expenditure, which is a major benefit for many chief security officers.

The great news is that intelligence is not an expensive thing to have. Although it requires people, process, and technology working in harmony, throughout this book I have striven to show that this does not require much expenditure. Technology is nice to have, but processes are free. Several are in this book, so you're already most of the way there! The big investment is therefore people, especially as the larger the team, the greater is the quality of the analytical output—and the more the bandwidth for supporting the business. There are clear economies of scale here, although of course the reality is that one needs to start slowly and build on proven success.

So, now that you've read this far, it's time to take action. If you're a corporate security professional, consider how you could take a better intelligence-led approach. This may not mean rolling out a new function; instead, it could be as simple as structuring what you're doubtless already doing to better understand your environment. Consider maintaining a list of IRs; setting up a consolidated list of sources, with notes, that you've set up to "push" to you; setting aside time to read these; having a system to store the most interesting snippets; and making time to write up and send out something on the security topic of interest to a key and ever-growing audience. You may be surprised at the interest and the results. Alternatively, if you're looking to set up a full function, then draw on the Estimate in the previous chapter: This is a virtual blueprint built on the blood, sweat, and tears of others, so you don't have to expend yours. Finally, if you're an analyst, researcher, collator, or intelligence manager, then hopefully you've taken away a few snippets of relevance to your corporate environment and, at the very least, have had a few ideas sparked from the text. We can all do things better, and we all know that the intelligence track is paved with hazards and slips, trips, and falls, so perhaps a few of the points will have been useful reminders for you.

Finally, of course, help spread the good word! After all, who would want unintelligent security driving their business?

REFERENCES

Accenture. 2012. *Managing political risk*

Controlling loss, finding opportunity. http://www.accenture.com/us-en/Pages/insight-managing-political-risk-controlling-loss-finding-opportunity.aspx

ACPO. 2010. *Guidance on the management of police information*. 2nd. ed. London: National Policing Improvement Agency. http://www.acpo.police.uk/documents/information/2010/201004INFMOPI01.pdf

AFRL. 2004. *Link analysis workbench*. Rome, NY: Air Force Research Laboratory Information Directorate.

Andrienko, Gennady, and Natalia Andrienko. 2009. Interactive cluster analysis of diverse types of spatiotemporal data. *SIGKDD Explorations Newsletter* 11 (2): 19–28.

Bergman, Michael. 2001. The Deep Web: Surfacing the hidden value. *Journal of Electronic Publishing* 7 (1). http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main

Berkowitz, Philip, and Michael Congiu. 2011. *The Littler report: Managing the global workforce—A legal and practical guide to dangerous international employee assignments*. http://www.littler.com/files/press/pdf/WP_IntlAssignments_2-23-11.pdf

Bonner Network Wiki. 2013. *Power mapping: A tool for utilizing networks*. http://bonnernetwork.pbworks.com/f/BonCurPowerMapping.pdf

Briggs, Rachel, and Charlie Edwards. (2006). The business of resilience: Corporate security for the 21st century. London: Demos.

Carter, David. 2004. *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. http://www.fas.org/irp/agency/doj/lei/guide.pdf

CIAB. 2013. *US economic sanctions laws and how they affect insurance brokers*. Council of Insurance Agents and Brokers. https://www.ciab.com/WorkArea/DownloadAsset.aspx?id=1212&libID=1234

Clark, Robert. 2003. *Intelligence analysis: A target-centric approach*. Washington, DC: CQ Press.

Claus, Lizbeth. 2009. *Duty of care of employers for protecting international assignees, their dependents, and international business travelers*. International SOS. https://www.internationalsos.com/en/files/Duty_of_Care_whitepaper.pdf

———. 2010. Duty of care of employers for protecting international assignees. *Effectif* 2010 (September–October): 21–23. http://www.rh2010.com/bilan2010/pdf/32a35_Claus_v13n4-en.pdf

Cooper, Jeffery. Curing Analytic Pathologies, Center for the Study of Intelligence, December 2005. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/curing-analytic-pathologies-pathways-to-improved-intelligence-analysis-1/analytic_pathologies_report.pdf

Cruz, Albert. 2006. *Crime scene intelligence: An experiment in forensic entomology*. Washington, DC: National Defense Intelligence College.

Davis, Jack. 1997. *A compendium of analytic tradecraft notes*. Langley, VA: CIA Directorate of Intelligence. http://www.oss.net/dynamaster/file_archive/040319/cb27cc09c84d056b66616b4da5c02a4d/OSS2000-01-23.pdf

Dechert, LLP. 2012. Compliance with international sanctions: "Facilitation" and "circumvention"—Considerations for EU citizens and US nationals wherever they are located. *Dechert on Point* 2012 (10).

de Geus, Arie. 1992. Modelling to predict or learn? *European Journal of Operational Research* 59 (1): 1–5.

Economist Intelligence Unit. 2005. *The importance of corporate responsibility*. http://graphics.eiu.com/files/ad_pdfs/eiuOracle_CorporateResponsibility_WP.pdf

Equality and Human Rights Commission. 2012. *Article 8: The right to respect for private and family life, home and correspondence*. London.

Factiva. 2012. *Information overload and the information professional*. www.factiva.com/campaigns/2012/1784

FBI. 2013. *Intelligence collection disciplines*. Washington, DC: Federal Bureau of Investigation Directorate of Intelligence. http://www.fbi.gov/about-us/intelligence/disciplines

Ford, Andrew. 2003. *Intelligence tradecraft and technologies: Where do librarians fit in*? Information Online 11th Exhibition and Conference.

Friedland, LeeEllen, Gary Shaeff, and Jessica Glicken Turnley. 2006. *Socio-cultural perspectives: A new intelligence paradigm*. McLean, VA: The Mitre Corp.

Gilbert, Michael, and Mauricio Espana. 2012. Due diligence: Critical steps to take and questions to ask when conducting pre-merger anti-corruption due diligence. *FCPA Report* 1 (5).

Glass, Roger, and Philip Davidson. 1948. *Intelligence is for commanders*. Harrisburg, PA: Military Service Publishing.

Gosden, Emily. 2013. Corporate manslaughter cases rise. *The Telegraph*, January 28.

Grau, Lester. 2004. *Something old, something new: Guerrillas, terrorists, and intelligence analysis*. Fort Leavenworth, KS: Army Combined Arms Center.

Gray, David, and Chris Slade. 2008. Applying the intelligence cycle model to counterterrorism intelligence for Homeland Security. *European Journal of Scientific Research* 24 (4): 498.

Helms, Dan. 1999. *The use of dynamic spatio-temporal analytical techniques to resolve emergent crime series*. Las Vegas, NV: Las Vegas Metropolitan Police Department.

Heuer, Richard. 1999. *Psychology of intelligence analysis*. Langley, VA: CIA Center for the Study of Intelligence.

Hollywood, John, Diane Snyder, Kenneth McKay, and John Boon. 2004. *Out of the ordinary: Finding hidden threats by analyzing unusual behavior*. Santa Monica, CA: RAND Corp.

Howell, Lee. 2013. *Global risks 2013*. Geneva, Switzerland: World Economic Forum.

Hughes Parker, Rebecca, and James Freis Jr. 2013. Anti-money laundering *FCPA Report* 2 (3).

Hulnick, Arthur. 2006. What's wrong with the intelligence cycle? *Intelligence and National Security* 21 (6): 959–79.

ICRC. 2009. *The Montreux document: On pertinent legal obligations and good practices for states related to operations of private military and security companies during armed conflict*. Geneva, Switzerland: International Committee of the Red Cross.

Institutional Asset Manager. 2012. *Asset managers should review bribery and corruption compliance, says Dechert*. http://www.institutionalassetmanager.co.uk/2012/11/29/177001/asset-managers-should-review-bribery-and-corruption-compliance-says-dechert

Interagency Threat Assessment and Coordination Group. 2009. *Intelligence guide for first responders*. http://www.ise.gov/docs/ITACG_Guide.pdf

International Association of Crime Analysts. 2002. *Identifying crime patterns*. http://www.iaca.net/Resources/Articles/identifyingcrimepatterns.pdf

Janco Associates, Inc. 2005. *Security manual template*. http://www.e-janco.com/Security.htm

Jensen, Carl J. III, David H. McElreath, and Melissa Graves. 2012. *Introduction to intelligence studies*. Boca Raton, FL: CRC Press.

Johnston, Rob. 2003. Foundations for meta-analysis: Developing a taxonomy of intelligence analysis variables. *CIA Studies in Intelligence* 47 (3): 61–71.

Joint Chiefs of Staff. 2000. *Joint publication 2-0 doctrine for intelligence support to joint operations*. Washington, DC.

Kapow Software. 2011. *Building your OSINT capability*. White paper.

Kopal, Robert. 2010. *The role of the criminal intelligence analysis in anti-terrorism*. Croatian Ministry of the Interior Crime Analysis Department.

Krebs, Valdis. 2002. Uncloaking terrorist networks. *First Monday* 7 (4).

Krizan, Lisa. 1999. *Intelligence essentials for everyone*. Washington, DC: Joint Military Intelligence College.

LeGault, Michael. 2006. *Think: Why Crucial Decisions Can't Be Made in the Blink of an Eye*. New York: Threshold Edition.

Lindberg, B.C. 1996. *Culture: A neglected aspect of war*. http://www.au.af.mil/au/awc/awcgate/usmc/lindberg.htm

Livingston, Robert. 1990. *Low-intensity conflict intelligence: Lessons from Vietnam*. US Department of the Army.

Lloyds. 2012a. *Market bulletin: Sanctions compliance: Due diligence guidance for the Lloyd's Market*. http://www.lloyds.com/~/media/Files/The%20Market/Communications/Market%20Bulletins/2012/02/Y4560.pdf

———. 2012b. *Sanctions due diligence guidance for the Lloyd's Market*. http://www.lloyds.com/~/media/Files/The%20Market/Communications/Key%20regulatory%20projects/Financial%20Crime/20120206_Sanctions_due_diligence_guidance.pdf

Luhn, H. P. 1958. A business intelligence system. *IBM Journal of Research and Development* 2 (4): 314.

Lum, Zachary. 1998. The measure of MASINT. *Journal of Electronic Defense* 8 (August): 43.

Mathiason, Garry, Peter Susser, Barry Hartstein, and Michael Congiu. 2012. *The Littler Report: The 2011 global employer—Highlights of Litter's Fourth Annual Global Employer Institute*. http://www.littler.com/files/press/related-files/Littler-Report-2011-Global-Employer-Highlights.pdf

McDowell, Don. 2000. *Strategic intelligence & analysis*. Pambula, Australia: The Intelligence Study Centre.Medina, Carmen. 2001. The coming revolution in intelligence analysis: What to do when traditional models fail. *Studies in Intelligence* 46 (3): 23–28.

Mercardo, Stephen. 2001. FBIS against the axis, 1941–1945: Open source intelligence from the airwaves. *Studies in Intelligence* 46 (11): 33-43.

———. 2005. Sailing the sea of OSINT in the Information Age. *Studies in Intelligence* 48 (3): 45–55.

Metscher, Robert, and Brion Gilbride. 2005. *Intelligence as an investigative function*. Tampa, FL: International Foundation for Protection Officers.

Ministry of Defence. 1998. *Joint warfare publication 3-50: Peace support operations*. Joint Doctrine and Concepts Centre.

———. 2000. *Joint warfare publication 2-00: Joint operational intelligence*. Joint Doctrine and Concepts Centre.

———. 2002. *Joint warfare publication 3-80: Information operations*. Joint Doctrine and Concepts Centre.

Moore, David. 2007. *Critical thinking and intelligence analysis*. Washington, DC: Center for Strategic Intelligence Research, National Defense Intelligence College.

Multilateral Investment Guarantee Agency, Japan Environmental Social Challenges Fund, Anvil Mining. 2008. *The voluntary principles on security and human rights: An implementation toolkit for major project sites*. Working paper.

NATO. 2001. *NATO open source intelligence handbook*. Brussels.

———. 2002a. *NATO open source intelligence reader*. Brussels.

———. 2002b. *AJP 2.1: Intelligence procedures*. Brussels.

———. 2002c. *Intelligence exploitation of the Internet*. Brussels.

Omand, David. 2010. *Securing the state*. London: C. Hurst & Co.

Osajda, Michael. 2010. *The FCPA and why it matters*. World-Check white paper.

PricewaterhouseCoopers. 2006. *Integrating political risk into enterprise risk management*. http://www.pwc.com/gx/en/political-risk-consulting-services/integrating-poitical-risk-into-enterprise-risk-management.jhtml

PRS Group. 2013. *International country risk guide methodology*. http://www.prsgroup.com/ICRG_methodology.aspx

Raghuvanshi, Vivek. 2010. *Information collection in corporate warfare*. http://corporaterisks.info/blog/?p=693

Renfroe, Nancy, and Joseph Smith. 2011. *Threat/vulnerability assessments and risk analysis*. http://www.wbdg.org/resources/riskanalysis.php?r=parking

Renzi, Fred. 2006. Networks: Terra incognita and the case for ethnographic intelligence. *Military Review* 86 (5): 16–22.

Rowley, Jennifer. 2007. The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science* 33 (2): 163–80.

Sabherwal, R., and I. Becerra-Fernandez. 2011. *Business Intelligence*, iii. New York: John Wiley & Sons.
Santini, Simeone, and Amarnath Gupta. 2002. Principles of schema design for multimedia databases. *IEEE Transactions on Multimedia* 4 (2): 248–59.
Schoemaker, Paul. 2012. *Profiting from uncertainty: Strategies for succeeding no matter what the future brings*. New York: Simon and Schuster.
Sims, Jennifer. 2010. Decision advantage and the nature of intelligence analysis. In *The Oxford Handbook of National Security Intelligence*, ed. Lock Johnson. Oxford: Oxford University Press.
Sinclair, Robert. 2010. *Thinking and writing: Cognitive science and intelligence analysis*. Washington, DC: Center for the Study of Intelligence.
Smith, Daniel. 2006. *Intelligence gathering in a counterinsurgency*. Carlisle Barracks, PA: US Army War College.
Sun Tzu. 1910/2009. *Sun Tzu on the art of war*. Trans. Lionel Giles. Pax Liborum.
Taleb, Nicholas. 2007. *The black swan: The impact of the highly improbable*. London: Penguin.
Travel Risk Solutions. 2012. *Legal obligations*. http://travelrisksolutions.com/legal-obligations
Troy, T. F. 1991. The "correct" definition of intelligence. *International Journal of Intelligence and CounterIntelligence* 5 (4): 447.
United States Army Intelligence and Security Command. 2003. *Open source intelligence operations handbook*. Washington, DC.
United States Department of the Army. 1989. *Study manual: Handling of sources*. http://www.soaw.org/component/content/article/46
———. 1990. *FM 34-3: Intelligence analysis*. Washington, DC.
———. 1994. *FM 34-130: Intelligence preparation of the battlefield*. Washington, DC.
———. 1998. *FM 34-8-2: Intelligence officer's handbook*. Washington, DC.
———. 2004a. *FM 2-0: Intelligence*. Washington, DC.
———. 2004b. *FM 3-07.22: Counterinsurgency operations*. Washington, DC.
———. 2005. *FM 3-19.15: Civil disturbance operations*. Washington, DC.
———. 2006a. *FMI 5-0.1: The operations process*. Washington, DC.
———. 2006b. *FM 3-19.50: Police intelligence operations*. Washington, DC.
———. 2006c. *FM 2-22.3: Human intelligence collector operations*. Washington, DC.
———. 2006d. *FM 2-22.9: Open source intelligence*. Washington, DC.
United State Department of Justice. 2001. *Department of Justice guidelines regarding the use of confidential informants*. http://www.justice.gov/ag/readingroom/ciguidelines.htm
———. 2005a. *Fusion center guidelines: Developing and sharing information and intelligence in a new world*. Washington, DC: Bureau of Justice Assistance.
———. 2005b. *Intelligence-led policing: The new intelligence architecture*. Washington, DC: Bureau of Justice Assistance.
———. 2006. *Analyst toolbox: A toolbox for the intelligence analyst*. Washington, DC: Bureau of Justice Assistance.
———. 2011. *The Bribery Act 2010: Guidance*. www.justice.gov.uk/guidance/bribery.htm

———. 2013. *A resource guide to the US Foreign Corrupt Practices Act*. http://www.justice.gov/criminal/fraud/fcpa/guide.pdf

University of North Dakota. 2009. *Using Excel as a database*. http://www.und.edu/dept/cndtrain/Excel/database.pdf

Voluntary Principles on Security and Human Rights. 2000. *The voluntary principles on security and human rights*. http://www.voluntaryprinciples.org

Von Clausewitz, Carl. 2013. *On war*. Trans. J. J. Graham. New York: Skyhorse Publishing.

Warner, Michael. 2002. Wanted: A definition of intelligence. *Studies in Intelligence* 46 (3): 15–22.

Watanabe, Frank. 1997. How to succeed in the DI: Fifteen axioms for intelligence analysis. *CIA Studies in Intelligence* 1 (1).

Wheaton, K. J., and M. T. Beerbower. 2006. Towards a new definition of intelligence. *Stanford Law & Policy Review* 17 (2): 329.

Wilson, Gary, Greg Wilcox, and Chet Richards. 2004. *Fourth generation warfare and OODA loop implications of the Iraqi insurgency*. 16th Annual AWV Strategy Conference.

Wilson, Michael. 2001. *Toward an ontology of integrated intelligence & conflict: A primer*. Decision Support Systems, Inc.

Case Law References

ABC News InterContinental Inc. v. Gizbert. 2006. No. 0160/06. UK Employment Appeal Tribunal.

Curtis v. Beatrice Foods Co. 1980. No. 78/1316, United States District Court, Southern District of New York.

Hicks v. Waterman Steamship Corporation and Maersk Line, Ltd. 2009. United States District Court, Southern District of Texas.

Khan v. Parsons Global Services Ltd. 2005. No. 04/7162, United States Court of Appeals, District of Columbia Circuit.

Longworth v. Coppas International (U.K.) Ltd. 1984. SLT 111, Outer House.

Palfrey v. ARC Offshore Ltd. and others. 2001. No. 304, Queen's Bench Division.

Preston et al. v. Tenet Healthsystem Memorial Medical Center, Inc. d/b/a Memorial Medical Center. 2011. No. 2006/10210, Civil District Court for the Parish of Orleans, Louisiana.

Saint Lo Tribunal des Affaires de Sécurité Sociale (Saint Lo Court for Social Security Cases) v. Directions des Constructions Navales (DCN). 2004. No. 203/00/366.

Waterman Steamship Corporation and Maersk Line, Ltd. v. Ruiz, Cronan, and Hicks. 2011. No. 10/516, Court of Appeals of Texas, Houston (1st District).

Statute Law References

European Convention on Human Rights. 1950. http://www.echr.coe.int/Documents/Convention_ENG.pdf

European Economic Community. 1989. *Council directive on the introduction of measures to encourage improvements in the safety and health of workers at work*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1989L0391:20081211:EN:PDF

European Union. 1996. *Directive 96/71/EC of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0071:en:HTML

ILO. 2006. *Convention C187: Promotional framework for Occupational Safety and Health Convention*. International Labour Organization https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312332

UK Bribery Act. 2010. http://www.legislation.gov.uk/ukpga/2010/23/contents

UK Computer Misuse Act. 1990. http://www.legislation.gov.uk/ukpga/1990/18/contents

UK Corporate Manslaughter and Corporate Homicide Act. 2007. http://www.legislation.gov.uk/ukpga/2007/19/contents

UK Data Protection Act. 1998. http://www.legislation.gov.uk/ukpga/1998/29/contents

UK Freedom of Information Act. 2000. http://www.legislation.gov.uk/ukpga/2000/36/contents

UK Health and Safety at Work Act. 1974. http://www.legislation.gov.uk/ukpga/1974/37

UK Human Rights Act. 1998. http://www.legislation.gov.uk/ukpga/1998/42/contents

UK Regulation of Investigatory Powers Act. 2000. http://www.legislation.gov.uk/ukpga/2000/23/contents

US Foreign Corrupt Practices Act. 1977. http://www.justice.gov/criminal/fraud/fcpa/docs/fcpa-english.pdf

US Occupational Safety and Health Administration Act. 1970. https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=OSHACT&p_id=2743

INDEX

G

H

I

J

K

L

M

N

O

S