2

The Biosecurity Threat Environment

Before we can really understand the role of intelligence in understanding and managing bio-threats, it is critical first to step back and assess the biosecurity environment. As discussed in Chapter 1, an important defining feature of intelligence—indeed a core function of any intelligence capability (both the human and processes) is how effectively does it 'tap into' the relevant security environment. The security environment can be defined as the sum total of threats and risks that any intelligence capability must understand as fully as possible if it is to reduce uncertainty and provide warning to decision-makers. Depending on the context, the security environment can be made up of a multitudinous and diverse number of threats and risks. For example, if you are a local police officer, your priority is to understand a security environment that most likely is made up of high volume crime issues, domestic violence and small scale drug offences. In contrast, if you are a WMD analyst in the CIA you will clearly not be interested in understanding local community threats and risks. Instead you will be looking at broader and deeper issues related to WMD proliferation, including: countries of concern, treaty compliance and evidence that terrorists groups may have the intent and capability to use WMD.

P. F. Walsh, *Intelligence, Biosecurity and Bioterrorism*,
https://doi.org/10.1057/978-1-137-51700-5_2

The purpose of this chapter therefore, is to map both the contemporary and emerging dimensions of the biosecurity environment. By doing so the chapter will address the first key objective of the book: *to provide an assessment of the contemporary (post 2001) and emerging biosecurity and bioterrorism threat environment.* With this achieved, it will provide us with a critical foundation in which to address the book's remaining objectives which seek to evaluate the role of intelligence in supporting decision-making in contemporary and emerging bio-threats, explore the effectiveness of intelligence processes and capabilities and understanding how intelligence can assist in both the management of unfolding and emerging bio-threats.

This chapter will survey the biosecurity threat environment in the following three sub-sections: *past, present and future.* As discussed in Chapter 1, the book's focus is assessing bio-threats from the present (defined as from 2001) to the future. The rationale for this approach is explained shortly, but in order to provide context for a detailed discussion of current and future threats, we will commence our discussion profiling very briefly bio-threats from 1945 to 2001. The brevity of this discussion is not to suggest that the period (1945–2001) was not important to shaping our understanding of bio-threats—indeed they have been crucial, rather it is because this period has been extensively covered already in the literature.

The smaller attention on this period (1945–2001) also does not imply all the complexity of past events and threats have been completely revealed or understood. There remains much to learn about past events that can inform current practice. The intention here though is to provide maximum space to surveying current and emerging threats—given understanding these remains a bigger and more immediate challenge for intelligence and policy-makers.

Defining 'The Biosecurity Threat Environment'

Before I move on to surveying the biosecurity threat environment, an important theoretical issue needs addressing. It is important because as we shall see in discussion below, there are a number of perspectives

used in scholarly work on biosecurity, intelligence and national security issues when describing and understanding what is labelled 'a threat'. In this book, I do not take a prescriptive approach to one theoretical perspective over another. Like many other areas in social science disciplines, different perspectives used together often provide a more global understanding of complex socially constructed issues such as what constitutes a 'bio-threat'? So it is important briefly here to reflect on two theoretical perspectives, which I argue are relevant to how scholars, intelligence analysts, and policy makers determine what constitutes a 'bio-threat'.

The two perspectives I will discuss here are realism and constructivism as they seem to have relevance to how intelligence agencies, governments and scholars have thought about how bio-threats are produced, constructed, their implications and management. Naturally, one could argue that there are far more theoretical perspectives relevant to how bio-threats have been constructed such as: liberalists perspectives, critical security studies, and social constructivism, but this is not a book on international relations theory and we will restrict discussions to realism and constructivism.

Classical realists perspectives tend to emphasise that in the absence of any global government it is anarchy, which shapes international relations between states. In a chaotic world—one with few binding laws, states seek security from others. This creates competition for power, which in turn determines the structure of the international system. State survival is therefore inherently a contest between states not internal threats (see Morgenthau 1967; Mearsheimer 2001; Waltz 1979). This approach was later 'softened' somewhat with the emergence of another generation of IR scholars (neo-realists), who while agreeing with their traditional realist colleagues that the international system defines how states behave, also saw domestic factors relevant to how states respond to each other (Burchill et al. 1996: 87–90).

Realist perspectives are useful to some extent in explaining some of the strategic decision-making used to generate state based bio-warfare programs particularly between Cold War opponents the Soviet Union and USA. Though realism is not solely adequate to understand a range of national security policy making on managing evolving bio-threats

after the Cold War ended. As noted later in this chapter, the biosecurity threat environment after the Cold War shifted away from an almost exclusive array of potential state based threats to an increasing number of non-state actor ones. This transition requires additional theoretical IR perspectives to make sense of the evolving threats and ensure that national security policy can also adapt to manage this new array of threats. Constructivist perspectives therefore are another useful approach in describing the post-Cold War bio-threat landscape because non-state actors such as bio-terrorists and their impact on the international system is not at its core a competition between states, but rather driven by group social construction and identity for influencing world politics (Wendt 1999).

In summary, many IR theories may be helpful in understanding past, current and emerging bio-threats including both realist and constructivist arguments. Throughout the book other IR theories (e.g. human security) are also used to expand the reader's perspectives on how to understand past and emerging bio-threats. As a result, I do not take a prescriptive view of one theory over another and only suggest the ones discussed here are one of many tools to help us better understand the bio-threat environment and what the intelligence and policy response might be. I will not spend any more time on a detailed analysis of IR theory as this is not germane to the book's objectives outlined in Chapter 1. What is important in applying any theoretical and analytical perspectives is that they need to help intelligence analysts more deeply deconstruct the nature of bio-threats in order to better understand how they may develop. In particular, as we shall see in Chapter 5, effective intelligence analysis (especially at strategic level) requires analysts to weigh both the probability and impact of various drivers for a bio-threat. In other words, an analyst needs to understand the significance of various factors (drivers) that might enable a bio-threat. Depending on the nature of the bio-threat, they need to assess the role of multiple drivers: technology, political instability, psycho-social issues, radicalisation, legislative and policy influences. Theoretical perspectives from IR, security studies and criminology to name only a few can help analysts identify drivers.

Past Biosecurity Threat Environment (1945–2001)

With biosecurity defined, this section will provide a brief historical overview of the threat landscape in the post-World War II and Cold War (1945–1991) period. An analysis of how bio-threats evolved during this period helps explain how the current policy focus arose post 9/11. As I have discussed elsewhere (Walsh 2014: 837–856), starting a survey of bio-threats at 1945 may seem a bit arbitrary given historians and scientists remind us that diseases whether naturally occurring or used as 'weapons' have for centuries had a major impact on the political and cultural history of humans (McNeil 1998; Crawford 2007). The year 1945, however, parallels the development of modern microbiology and the ability by states to use technology to 'industrialize' various biological agents as weapons. Although Germany and Japan during World War I had biological weapons production capabilities, the delivery of such weapons were rudimentary. At the end of World War II, however, developments in industrial microbiology and advances in the aerolisation of biological agents made weaponising them a more accurate and lethal option for states that choose to develop them (Geissler and van Courtland Moon 1999; Walsh 2014; Spiers 2010).

State based biological weapons programmes, particularly those developed by Cold War protagonists—the former USSR and USA from 1945 until 1970s (for the USA), and up to the 1990s for the Soviet Union, dominated policy maker's understanding and framing of the bio-threat environment. Other US allies such as the UK and Canada also had invested heavily in offensive biological weapons programmes (Spiers 2010; Balmer 2001; Regis 1999; Carus 2017). For example, the UK developed its own capability in the 1930s, but abandoned it as a retaliatory option in 1957 (Spiers 2010: 56; Balmer 2001). These were large, industrial programmes that produced vast quantities of dangerous pathogens, such as highly virulent anthrax, plague and tularemia.[1] Prior to President Nixon terminating the US offensive bioweapons program, the US Army had weaponised two lethal agents (*Bacillus anthracis* and *Francisella tularensis*) and three incapacitating biological agents, *Brucella*

suis, Coxiella burnetti, and Venezuelen equine encephalitis virus (VEE). Supplies of these agents had been mass produced and were stockpiled at the Army's Directorate of Biological Operations at Pine Bluff Arsenal, Arkansas (Regis 1999: 210). According to Regis, the production plant had an overall capacity of 86,000 gallons (ibid.: 211). The Pine Bluff facility fermenter was smaller than an older Vigo plant in Indiana, which had a capacity of 240,000 gallons, but nevertheless could produce a substantial amount of agent (Regis 1999: 211). The Soviet Union built large bioweapons plants in Sverdlovsk (1946), Kirov (1953) and others such as the one in Stepnogorsk (in Kazakhstan), which was under the control of the ministry of defence and Biopreparat Group (a civilian pharmaceutical agency). At the time, US intelligence knew little about the extent of these programmes and it wasn't until the defection of Ken Alibek (chief scientist and deputy director of Biopreporat) and biologist Vladamir Pasechnik to Britain in 1989 that the US and other NATO allies knew the full extent of the Soviet programme (Spiers 2010: 62). For example, according to Ken Alibek's account of his time as the chief scientist of the Soviet biological weapons, just one of its six biological weapons production facilities at Stepnogorsk (in Kazakhstan) contained ten 20,000 litre fermenters capable of producing 1000 tonnes of anthrax per year (Alibek 1999: 229–301). By the late 1960s at the time that US President Nixon announced a termination of an offensive American bioweapons programme, the US military had developed 'a biological arsenal that included numerous bacterial pathogens, toxins and fungal plant pathogens that could be directed against crops to induce crop failure and famine' (Christopher et al. 1997: 417). The UK's and later US abandonment of an offensive biological warfare programme, however, had been based on a calculus by policy makers in London and Washington that the growing power of atomic weapons offered a more reliable offensive option than a biological bomb (Balmer 2001: 157). There were a number of drivers influencing a shift away from an offensive state based biological weapons programme in the US and UK. Additionally, by 1960s 'the nature of the threat changed as a complex mixture of technical, economic, political and legal considerations combined to provide for successive changes in outlook' (Balmer 2001: 184). There were variations within policy circles about the

immediacy of the threat from state based biological weapons programs (ibid.: 184) and biological weapons once firmly seen in the same way as chemical and nuclear weapons of mass destruction begun to be seen differently by policy makers. Biological weapons lost the status of offensive weapons of mass destruction and along with this the loss of resources. Concern however, was also raised from 1945, and during the Cold War, that other less stable or rogue states (Iraq, Iran, Syria and North Korea) were seeking to develop biological weapons (Koblentz 2009: 17–18; Spiers 2010: 102–125). Though in some cases, such as Syria information about biological weapons programs was sketchy and lacked specificity (Zanders 2015: 152).

The major exception was Iraq. Iraq in particular showed an early interest (as far back as 1974) in developing biological weapons for their strategic deterrent value. By 1990, the Hussein regime had tested and weaponised anthrax and botulinum toxin using 400 kilogram aerial bombs and Al Hussein warheads. Though thankfully these were not very efficient for disseminating biological weapons and the regime never produced dried, powder agents, which could have covered greater differences and potentially had more lethality (UNMOVIC 2007: 768–790). By the end of the first Gulf War in 1991, as UN weapon teams moved into Iraq, the Iraqi regime destroyed its bulk supply of biological agents and munitions (Walsh 2014).

During the mid-1990s, policy makers started to shift their focus from historical and traditional notions of bio-threats (state sponsored conventional biological weapons programs) to the use of biological agents by non-state actors—primarily terrorists (Koblentz 2009: 200–227). There are a number of policy and changes in the security environment, which underpinned this shift in attention of policy makers away from the traditional state based and military application of biological weapons dominating their attention up until the end of the Cold War. First was a concern that the fall of the Soviet Union and the immediate decline in Russia's economy in the 1990s would see a lot of unemployed bioweapons scientists as 'guns for hire' by terrorists and other rogue states. Another event (discussed in more detail below) was the 1995 Aum Shinrikyo subway attack in Tokyo, the 1993 attack on the World Trade Center in New York and the 1996 terrorist attack in Oklahoma city all

made clear to policy makers, Gronvall argues that the United States was vulnerable to terrorism and the implication that some groups might use biological weapons (Gronvall 2012: Chapter 1). At the same time too, by the late 1990s, increasing developments in biotechnology and the biomedical sciences such as the human genome project raised concerns by some policy makers that such technology in the wrong hands could result in catastrophic bio-attacks (NRC 2004). In particular, the Bush Administration made several announcements that rogue states and terrorists posses bioweapons and are willing to use them (Spiers 2010: 164). The Administration also expressed concerns publicly that advances in biotechnology and life sciences would result in the creation by adversaries of new novel bioweapons that would require 'new detection methods preventive measures and treatments' (Spiers 2010: 156). In April 2005, the Administration said: 'these trends increase the risk for surprise. Anticipating such threats through intelligence efforts is made more difficult by the dual use nature of biotechnologies and infrastructure and the likelihood that adversaries will use denial and deception to conceal their illicit activities' (Spiers 2010: 156). Even after the faulty intelligence on Iraq's possession of WMD which led to the US led invasion of Iraq in 2003 was revealed, other senior US legislators still underlined their assessments that the threat from biological weapons was growing and that genetic modification techniques would 'allow the creation of even worse biological weapons' (Silberman and Robb 2005: 34). Further discussion below and in Chapter 5, argues that the policy pronouncements on the dangers of non-state actors using or developing bio-weapons throughout the period 1999–2009 was not based on 'sophisticated threat assessments' and for many researchers in the field was 'systematically and deliberately being exaggerated' (Leitenberg 2005: 88).

Koblentz (2009) provides a useful summary explaining how 'bio-terrorism' became the policy priority during this period, which in turn redefined the bio-threat space. There is insufficient space to discuss all the events responsible for this shift in policy interest, but we will discuss three significant ones here as they help provide a contextual understanding as to why political leaders started to shift their focus on bio-threat actors away from states to groups and even individuals.

The first event occurred in 1995 when the Japanese doomsday cult Aum Shinrikyo released sarin nerve gas into the Tokyo subway system killing 12 people and injuring 5000 more (Rosenau 2001; Leitenberg 1999: 151–153). As Rosenau notes, 'this attack marked a turning point in the history of terrorism as it was the first time, non-state groups had used chemical weapons against civilians' (2001: 289). While the attack was serious enough, investigations later revealed that the cult had also acquired anthrax and botulinum toxin and was attempting to weaponise it against various Japanese government political, military and public institutions. The cult failed to cultivate sufficiently lethal strains of botulinum toxin and anthrax. Its plans were foiled by other technical challenges, including not being able to disseminate anthrax into the appropriate aerolised and sized spores required to produce mass casualties (Leitenberg 1999). As Rosenau points out, despite the cult having the motivation and resources to use biological agents as weapons, they still lacked the full complement of 'scientific and technological skills that would have helped ensure their success' (Rosenau 2001: 296).

The second event which elevated the importance of bio-terrorism for policy-makers was discoveries by US soldiers post the 2001 invasion of Afghanistan of technical documents and equipment in a biological weapons laboratory under construction near Kandahar. Additional documents were also found in a close by al Qaida training camp—detailing the terrorists groups plans to develop a biological weapons capability. Since 1998, Osama Bin Laden had made statements that the 'acquisition of WMD was a 'religious duty' (Pita and Gunaratna 2009: 10). In his memoirs, former Director of the CIA, George Tenet mentions two individuals (Rauf Ahmad and Yazid Sufaat), who were recruited by al Qaida's second in charge Ayman al-Zawahiri to develop this capability. The documents and searches of the laboratory showed that the al Qaida program was in its early stages and the group had not yet obtained a virulent strain of anthrax or mastered the technique to aerolise it (Tenet 2007: 278–279).

The capture, interrogation or death of most of the key al Qaida operatives associated with its fledgling bio-weapons program constrained further efforts by the group to continue down this pathway. Though throughout the rest of the decade, policy makers and intelligence agencies remained concerned that 'al Qaida central' may have shared what

expertise it had developed with its other regional franchises throughout the world. For example, there is some evidence that through Al Qaida's many technical websites aimed at supporting the operational activities of jihadis around the world (e.g. the Mausu'at al-E'adad or the Preparation Encyclopedia) has shared some expertise about making biological weapons. Additionally, after the US led invasion of Iraq, coalition forces found a three volume manual outlining steps for conducting chemical and biological experiments in an area previously occupied by Al Qaida affiliate Ansar al-Islam in northern Iraq. There are other reports that Ansar al-Islam were reportedly engaged in the production of ricin, but there is no evidence that it reached a stage of large scale weaponisation that could cause mass casualties (Salama and Hansell 2005: 622). There remains however, little consistently compelling evidence that other al Qaida affiliated groups have developed either the intention or capability to develop biological weapons (Salama and Hansell 2005: 618; Tucker 2012).

Concerns also remained over the possibility that al Qaida franchises or 'do it yourself jihadists' would start developing biological weapons from the increasingly available 'recipes' for making them posted on the internet by other jihadists. These recipes were generally crude and unlikely to result in mass-casualties (Koblentz 2009: 223–224; Tucker 2012). In summary, what this second issue demonstrated was although there was a strong desire by al Qaida to develop biological weapons—the capability, particularly the resources, knowledge and skill sets to do so were in short supply. I will return to the importance of *knowledge and skill sets* to understanding biological threats later when discussing emerging threats. Another important aspect of this issue is that there were differences of opinion within the US intelligence community and among biodefense experts on how significant the level of threat and capabilities al Qaida was in bioweapons development pre the 2001 war and post the invasion of Afghanistan (Silberman and Robb 2005; Leitenberg 2005). We will turn back to these variations in analytical assessments in Chapter 5.

In contrast to al Qaida's general lack of advanced knowledge and skills in pursuing biological weapons, the third bio-terror event involved the 2001 release of anthrax spores in the US mail system, and showed

the lethality of biological agents when developed by individuals or groups, who do possess expertise to produce and weaponise dangerous pathogens. In September and October 2001, seven envelopes containing a dried powder form of anthrax spores were posted to several media outlets and to the US Senate offices of Senators Thomas Daschle and Patrick Leahy. The letters resulted in 22 cases of anthrax—five of which led to fatal inhalational anthrax. The anthrax letters also resulted in the contamination and closure of several major US postal offices.

In contrast to attempts made by Aum Shinrikyo and al Qaeda to use anthrax as biological weapons, the FBI investigation revealed that the anthrax used in this attack was a highly concentrated, aerolisable 'weapons grade' form of this bacteria. The subsequent seven year investigation was complex and protracted and resulted in the US Department of Justice determining that a single spore batch created by anthrax specialist Dr. Bruce E. Ivins at the US Army Medical Research Institute of Infectious Diseases (USAMRID) was the parent material for the letter spores. In July 2008, Ivins committed suicide before being indicted (Walsh 2011: 49).

Present Biosecurity Threat Environment (2001–Present)

The Ivins case was significant on a number of fronts. While it did not result in mass casualties (the mode of delivery via mail was not optimal for this), it did underline the tremendous skill required to produce biological agents in sufficient pure and aerolised quantities. Ivins had been an anthrax expert for over two decades yet the FBI case against him documents (despite his extensive knowledge and the optimal laboratory conditions), that he was confronted with challenges in producing the anthrax thought responsible for the attack (DOJ 2010). The anthrax incident was unsettling—coming only a week after the 9/11 attacks in New York. Though several facts of the Ivins case, in particular the challenges he faced in producing the anthrax helped re-calibrate some of the assessments being made in the intelligence community about how

easy it would be for non-state actors, such as al Qaida to produce and disseminate biological agents as weapons. This may have been comforting to some policy makers, though it did raise another bio-threat scenario—namely that that the terrorists may not be an outsider, but rather an insider—even more concerning a scientist capable of developing a biological weapon.

The fact that the 'attacker' had been a scientist with access to highly controlled dangerous biological agents focused intelligence agencies on the threats and risks associated with *dual-use research and technology*. More time will be spent on the significance of dual use research in the context of emerging bio-threats later on, but briefly dual use research and technology means activities, knowledge and equipment, which is used for legitimate research (for example the development of vaccines), but could also be used inappropriately by those motivated by politics or crime. It is assessing the significance of dual-use research and technology, which came into sharp focus during the *Amerithrax* incident that has dominated discussions about bio-threats in the present period.

Other biosecurity issues that have shaped the post 9/11 threat environment have included a litany of 'bio-crimes'. Bio-crimes as we discussed in Chapter 1 are a diverse bundle of issues, which have in common the use of biological agents as weapons by non-state actors for extortion, murder or profit rather than politically motivated reasons seen in bioterrorism. A 2001 study by Seth Carus attempted to delineate between the motives of bio-terrorists and bio-criminals by surveying major cases of each back to 1900. He concluded that in contrast to bio-terrorism, bio-criminal attacks tend to be aimed at individuals or small groups using crude means of dissemination (for example food contamination, murder of spouses using ricin, or illegal injection of pathogens (HIV) to a victim) (Carus 2001: 6–10). Other authors include politically motivated assassinations such as the famous case of Bulgarian writer and journalist Georgi Markov, who was executed by the Bulgarian secret police in London after he was stabbed in the thigh by an umbrella which discharged a ricin soaked pellet into his leg (Burnette 2013: 35–36). Burnette also includes the *Amerithrax* incident as an example of a bio-crime whereas others see this as an act of bio-terrorism (ibid.).

In reality however, there is still a 'lack of professional consensus' on the differences between these two threat classes and as noted earlier 'evolving perceptions of the threat' remain. Inglis and colleagues tend to lump a number of bio-threats across the bio-criminal and bio-terrorists space together. They refer to a 'cluster of malevolent criminal actors (bio-crime, bio-terrorism, deliberate biological release, biological-weapons of mass destruction, murder, homicide and grievous bodily harm with intent' (Inglis et al. 2011: 18).

The bio-criminal threat landscape however, has shifted since the 2011 study by Carus, which focused primarily on small individually motivated bio-attacks by criminals. While bio-criminals will continue to extort money or seek revenge on single victims using biological agents—global food quality, environmental pressures, and companies seeking to 'cut corners' present another layer of more complex bio-criminal threats in the future with potentially greater economic and public health impacts beyond individuals, to groups and nations. For example, an increasing number of recent incidents related to food production illustrate this sector's vulnerability to criminal exploitation. In China there have been several incidents of adulterated infant formula, including the 2008 case where a company used a sub-standard formula that included the industrial chemical melamine—resulting in six deaths and over 300,000 children with kidney disease (Yam 2013). In February, 2013, global food company—Findus—suffered major reputation damage after it was found that some of its ready to eat meat based products were 100% horse (Neville 2013). In August 2013, New Zealand dairy giant, Fonterra had to recall infant formula from Asian markets after it was discovered that some of its whey protein may have been contaminated with botulism (Trevett 2013). Similarly, in countries with large primary industry sectors such as Australia and New Zealand, the organized, criminal manipulation of regulations concerning export/import markets, or the criminal introduction of a controlled plant or animal species represent serious biosecurity threats to these economies.

Finally, a cluster of biosecurity issues, which arguably do not sit neatly under either the 'bio-terrorism' or 'bio-crime' classifiers have begun to capture the focus of policy makers post 9/11. Many of these, such as the

2003 SARS outbreak, the 2009 H1N1 influenza pandemic, the 2014 West African Ebola outbreak and 2015 expansion of the Zika virus into South America are more correctly viewed as public health emergencies, in that they were the result of natural causes and not the intentional or malevolent actions of threat actors.[2] Nevertheless, all these cases, had wider impacts beyond public health. They showed how the pathogen involved was zoonotic (i.e. had the ability to move from one species to another), and each impacted significantly on the global economy and wealth of nations. For example, SARS forced the closure of airports, reduced global travel and resulted increased sick days of many countries.[3] So in the broadest sense of what 'national security' means such pandemics, which can skip species, especially from animals to humans also have profound impacts on the economic security of nations.

As a result of some of these natural pandemics since 9/11, governments in Australia, Canada, New Zealand, the USA and UK also declared that a broader focus and inclusion of other non-bio-terror threats and risks was required. As suggested in Chapter 1, it was becoming clearer that in some cases, the biosecurity response to some of these problems was fragmented. Agricultural scientists, animal and human health specialists tended to only look at the risks posed by zoonotic diseases from their own perspective, but what was needed was a more joined up integrated approach to detecting and managing such pandemics that crossed species. In Australia, Canada and New Zealand, researchers and policy-makers started to refer to this needed policy response as a *one health approach* or *one health continuum* (Walsh 2011: 53–67).

It remains unclear however, the extent to which the rhetoric of a 'one health' response to pandemics has been implemented across agricultural, animal and human health government departments in these and other countries. This is an important discussion which will be developed further in subsequent chapters as it is directly relevant to how we can optimize the role of intelligence in the broader biosecurity context. But what is even less clear, is the extent to which health intelligence or epidemiology gathered about pandemics—which arise from cross species barriers—is fed into the national security intelligence communities of these countries to increase their understanding of naturally occurring pathogens that could be exploited by threat actors.

Emerging Biosecurity Threats (2018–2023)

Given the baseline survey of the post-9/11 bio-threats above, what types of threats and threat actors are likely to emerge over the next five to ten years? There is a great deal of uncertainty around what scientists and security specialist assess as emerging bio-threats. John Caves and Seth Carus' analysis of the future of weapons of mass destruction out to 2030 included a range of perspectives from other experts—many who came to the same conclusion that 'the pace of change is so great in life sciences that they cannot confidently predict where the technology would be in five years much less than in twenty years' (Caves and Carus 2014: 26). Caves and Carus conclude in their study that it is impossible to predict specific biological weapons capabilities available by 2030, but they do assess the growth in biological sciences means what will be possible will be much greater today, 'including in terms of discrimination and the ability to defeat existing defensive counter-measures' (ibid.). Interestingly Caves and Carus assess a number of existing capabilities that been around arguably for decades, which don't involve genetic manipulation or bio-engineering as being potentially exploited by terrorists: including using geo-tagged images from the internet to harvest pathogens from nature of virulent disease, selective culturing to identify strains that are especially virulent or more resistant to existing counter-measures using equipment such as bioreactors available over the internet. They also see the potential exploitation of commonly available agricultural sprayers that can enable high efficiency dissemination of liquid pathogen solutions without special adaptations (ibid.: 26–27). Caves and Carus also briefly discuss the development of new biological weapons, particularly production of viruses such as small pox that are not readily available in nature anymore through the exploitation of molecular modeling and engineering. They argue that the exploitation of this kind of technology will most likely occur in state programs though recognize that terrorists could also utilize it. Their assessment does not indicate which state and non-state actors are likely to exploit emerging bio-technology. It is not possible to provide a full account of all potential emerging bio-threats, so this section will provide a thematic list of major

ones. In reality, emerging threats do not fit into neat sub-categories and 'threat areas' can overlap each other. For example, a stolen biological agent from a secure biosafety rated government laboratory may also be a synthetically produced agent with dual-use properties (i.e. it can be used for legitimate scientific reasons but also illegitimate or illegal purposes).

With this caveat in mind, I see the following two biosecurity threat thematic areas as presenting challenges to intelligence agencies, policy makers and first responders in the future. The first theme is '*stolen biological agents*'—and includes material that has been stolen from a supplier, a university, research lab, hospital or animal health facilities. The second theme is '*dual-use research and synthetic biology*'. We will return to a further detailed discussion of these threat thematic areas in subsequent chapters but here we will provide a brief overview of them.

Turning first to 'stolen biological agents', the events of 9/11 and the anthrax letter attack discussed earlier resulted in a number of changes to policy, legislation and codes of ethics aimed at enhancing the control and access to dangerous biological agents and toxins in the USA. Similar policy initiatives have also been developed in other western nations such as Australia, Canada, UK, and the EU. We will come back to a more detailed discussion of policy initiatives in Chapter 8 and their influence on how intelligence supports and is influenced by policy in the biosecurity context. However, a brief discussion of some landmark policy initiatives is important here in order to understand what type of emerging bio-threats may be likely over the next five to ten years. While Chapter 8 will provide a more fulsome discussion of policy and legislative initiatives across other 'Five Eyes' countries, I will restrict the discussion here to key policy changes in the USA. This is because the USA has tended to lead other nations in developing biosecurity oversight policies—partly as a result of 9/11 and the anthrax letter attack.

Both of these events resulted in new policy and legislative provisions, which increased the oversight, control and access to dangerous biological materials. In particular, the enactment of the USA Patriot Act 2001 and the Public Health Security and Bio Terrorism Preparedness and Response Act 2002 required the registration of persons allowed to work with such agents (see in particular, Sections 201 and 351A, of the Act).

Further initiatives such as Biological Surety (US Army 2008), the National Academies Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology chaired by Gerald Fink[4] in 2004 also played a role in identifying internal risks posed by those working in secure laboratories (NRC 2004). These initiatives collectively provided guidance on how to improve internal oversight: including background checks on scientists as well, as other safety protocols that appropriately risk managed the access, production and transfer of dangerous pathogens. So it is important to understand how policy, legislative and accountability mechanisms have evolved and whether they decrease or increase vulnerabilities for threat actors to exploit within the biosciences enterprise.

Stolen Biological Agents

Leaving aside the investigation into microbiologist Bruce Ivins and the anthrax postal incident of 2001 discussed earlier, the 'insider threat' to date of a scientist stealing or conspiring to steal a controlled biological agent appears to be both really rare and extremely difficult to detect. Though there have been some cases. For example, a Japanese researcher stole data and material from his host lab (the Mayo Clinic) in 1999 (Cass 1999). Burnette (2013) and Salerno (2015) document others. The increased policy and biosafety regulatory environments that provide guidance on the design, construction and operations of BSL-3 and BSL-4 labs makes it more difficult now than in 2001—both for unintentional accidents in the workplace and the theft of pathogens. BSL-3 and BSL-4 labs are the two most secure bio-safety lab designations. In both cases, strict guidelines prescribe the physical layout, safety equipment and training of scientific staff, who work in them. In BSL-3 and BSL-4 rated labs, scientists work on pathogens that can cause serious or potentially lethal disease. Generally, the most lethal agents, where there is either no vaccine or an unknown risk of transmission are worked on in BSL-4 labs. Debates continue however, within the bureaucracies of western countries about whether biosafety standards for BSL-3 and BSL-4 labs are sufficient (see, for example, GAO 2013). In Chapter 7

(Intelligence and Stakeholders) we will return to a more detailed discussion of biosafety standards and 'the insider threat', but suffice it to say several accidents across 2014 and 2015 in the handling and transportation of dangerous pathogens by the CDC (H5N1 and anthrax) and the US Army (anthrax) involving high containment labs suggest that there is room for improvement in biosafety standards (Schnirring 2014; Burns 2015; Salerno 2015: 191–204). Despite all the new bio-safety measures that have been put in place since 9/11, it remains difficult to predict and detect if someone has the intent and capability to steal a biological agent from a secure lab site for profit, political motivation or due to a mental health issue.

Background checks on scientists may assist in flagging staff, who present security risks *prior* to their appointment—though this process cannot screen out completely individuals whose ethics and intentions change later in their careers in ways that present security challenges. The motivation for individuals to use criminally biological agents from secure labs will likely be different in individual cases. From a bio-criminal perspective, where profit reward is the motive, the intent to commit the theft also depends on the nature of the agent potentially available to the criminal conspirators and how quickly the act can be turned into a 'profit'. In most western countries such as Australia, Canada, New Zealand, UK and the US, stealing a controlled biological agent such as anthrax from a BSL-3 or BSL-4 private or government lab, while not impossible, presents a number of security challenges in terms of physical security barriers and exposure risks for a criminal gang interested in such an enterprise.

There theoretically *may* be some criminals interested in trading controlled biological agents like anthrax, tularemia, or the plague. Though as the 2001 Ivins case revealed, the genetic sequence analysis of the Ames strain of anthrax used in that attack, makes possible the tracing of some of these substances back to their source—enabling investigators to identify which laboratories they came from and ultimately who was working with them. This then becomes a high risk venture for the individual or any organized crime group involved. Even if crime groups have access to scientists or laboratories they may calculate that traditional sources of revenue such as drugs, fraud and money laundering

might be in comparison less riskier ways to make money. However, it is possible that for some criminal groups or a scientist working for a biotechnology company, intellectual property theft of new scientific breakthroughs may be more attractive financially, and logistically easier to commit then the theft of a controlled biological substance from a high containment lab. We know there is a long history of economic espionage particularly in the biotechnology sector. For example, there have been theft of trade secrets involving delivery of technologies for small interfering RNA molecules, potential treatment for Alzheimer disease and new immune suppressive drugs and the role of the 'insider' has been key to many of these. Theft of research data has also been common (Elliott 2007: 293; Cass 1999). Another dimension of theft of intellectual property from a research institution or biotechnology company is of course is the theft of data remotely as a type of cybercrime. While making threats to 'use' stolen biological agents as weapons may create the psychological terror sought after by terrorists, exacting harm on an innocent target can still be more efficiently and cheaply achieved using simple homemade devices—such as the kitchen pressure cookers used by the Tsarnaev brothers in the 2013 Boston bombings. Yet we cannot assume there will be no future interest and capability by non-state actors to steal dangerous biological substances or associated data from 'secure' biological facilities. Actual or potential vulnerabilities and attempts by threat actors to steal biological material and information will obviously need careful monitoring for their national security significance. Intelligence agencies need to keep an open mind yet one informed by evidence of whether future cases of theft from facilities might indicate a shift in our understanding of the threat trajectory by non-state actor individuals or groups. We saw during the rise of Islamic State (IS) how IS broke many of the rules that even AQ didn't step over.

While the physical IS Caliphate has largely been dissolved, the endemic instability in Syria and even in Iraq may create opportunities for other non-state actors to procure biological weapons from facilities where biosafety barriers are vulnerable either physically or virtually. We know that up until 2013 the Syrian government had the largest stockpile of chemical weapons in the Middle East and used chemical weapons (Sarin nerve agent) against its own civilians during the civil

war though the government in Damascus (Zanders 2015: 150–157). Syria has also still not ratified the 1972 Biological and Toxin Weapons Convention (BTWC), though there is no evidence that the regime has 'set up a full biological weapons program beyond some elementary research' (Zanders 2015: 152). While the ongoing conflict in Syria makes it a hostile location for a non-state actor to pursue the development of biological weapons there, the illicit transfer of scientific knowledge or materials could theoretically be on sale if the price is right.

In summary, the control of laboratories in developing countries *may* be more vulnerable to criminal exploitation if physical security is not optimal or scientists do not perceive that they are adequately remunerated for the research they do (Friedman 2015: 176–180). Vulnerable areas such as the Middle East have few regional institutions that can engage states on biological threats. Friedman provides the example of the Middle East Consortium on Infectious Disease Surveillance (MECIDS) composed of public health experts and ministry of health officials from Israel, Jordon and the Palestinian Authority has made some progress particularly during the 2009 H1N1 pandemic facilitating joint action. However, more efforts need to be made to build capability in the region to counter biological threats from any source—including identifying early signs of threats to physical security in biological facilities and greater cooperation between health and security officials within the region (Freidman 2015: 179).

In addition to difficulties assessing motivation, it is also impossible to measure the consequence of a theft of a Category A pathogen from a BSL-4 lab. Part of this difficulty goes back to motivation. Is the objective of the theft to merely pose a threat to a community or extort funds from a government without the intention to actually use the substance? Or is the intention that the pathogen is weaponised and disseminated at ports, truck stops or airports? Leaving aside issues such as atmospheric temperature, sunlight and choice of dissemination vehicle, there are also other variables at play, which impact on the overall pathogenicity and 'contagion dynamics' of dangerous pathogens into a locality. While there is an active research agenda into epidemiological modeling and surveillance it remains difficult to predict 'the likelihood of a global pandemic, and to mitigate its consequences' (Bombardt 2000; Stattner

et al. 2011; Nicolaides et al. 2012: 1; Goncalves et al. 2013; Bravata et al. 2004; May et al. 2009; Lucero et al. 2011). There are also remain a number of challenges at global, regional and local health levels on the storage, real-time sharing and coordination of epidemiologic and laboratory data that can be used for the surveillance of emerging pandemics. Challenges include sufficiently trained personnel to review data, bureaucratic distrusts between different authorities from different sectors and jurisdictions and inadequate laboratory and research capacity to fund pandemic preparedness and surveillance mechanisms. These challenges exist to greater and lesser degrees in developed and developing countries (Edge and Hoffman 2015: 157, 179) and will be discussed further in Chapter 7.

Dual Use Research and Synthetic Biology

Though the theft of well-known and controlled pathogens such as anthrax from a BSL-4 laboratory seems less likely (at least in the 'Five Eyes' countries), debates continue about how dual use research and synthetic biology might create a number of potential emerging threats, risks and vulnerabilities. Such threats may arise from two sources. First there are concerns that highly skilled and trained individuals could use their knowledge to create biological agents under the guise of legitimate research for illegitimate ends. The second source of concern is interested 'outsiders' exploiting legitimate advances in conventional biological research, synthetic biological sciences and bio-technology for illegitimate purposes. Both pathways to potentially new bio-threats underline concerns about dual use technology. Each pathway also defines the key dimensions of 'dual use research', but in reality there are many ways this term has been defined in science, policy and security circles (for example, see, McLeish and Nightingale 2007: 1636; Shea 2006, summary; Tucker 2012; Williams-Jones et al. 2014: 4). While the concept of dual use technology has been around in the arms control and military literature for decades, its application in the biosecurity context is comparably recent. Regardless of what definition of 'dual use research' one adopts, its application in the biosecurity context has largely focused on the

research of dangerous biological agents that might be weaponised, and the publication of that research, which theoretically could be disseminated to bio-criminals or terrorists for their own nefarious objectives.

In recent years, the published results of dual use research have captured the concern of the biosecurity policy community and the media—perhaps even more than the experiments the articles describe. Starting in the early 2000s, McLeish and Nightingale argue that the publication of three papers: 'one on the synthesis of polio virus cDNA without a natural template by Cello et al. (2002), the second on how the variola virus (small pox) can invade the immune system by Rosengard et al. (2002), and a third on overcoming resistance to mousepox by Jackson et al. (2001), were widely interpreted as publishing blueprints for terrorists and led to public calls for changes to research and publication procedures' (McLeish and Nightingale 2007: 1636).

Other publications, have followed such as the article detailing the reconstruction of an influenza virus with all the identified gene sequences of the 1918 influenza virus (Tumpey et al. 2005: 77–80), and a 2005 research article describing the potential impact of contaminating the milk supply with botulinum toxin (Wein and Liu 2005). Additionally, two separate articles one in 2012, and the other a letter in August 2013, also raised security concerns about dual use research, and whether the published outcomes of these could be used for illegitimate reasons such as bio-terrorism. The 2012 article showed how scientists were able to identify the genetic changes needed for the avian influenza H5N1 to be efficiently transmitted between ferrets—a surrogate for human to human transmission.

The US National Science Advisory Board for Biosecurity (NSABB) had to determine whether the benefits of such research outweighed the risk of the accidental or intentional release of a lethal new virus. In November 2011, the NSABB recommended that the two articles arising from this research be redacted. The Board also called for the papers data and methods to be shared only with approved scientists and clinicians. This was, as Maher comments, an odd position for US Government to be in as the NSABB was potentially censoring research that the government had funded (Maher 2012: 431).

The NSABB's initial decision was later over-turned with the Board recommending (though not unanimously) that both papers be published in March 2012. The H5N1 research article publication ordeal shows the ongoing challenges in both identifying and oversighting dual use research. The questions of what experiments may be too risky to do and publish and how governments effectively manage this risk remains unclear. In August 2013, twenty-two researchers from labs around the world—some associated with the H5N1 research discussed earlier—submitted a letter to the journals *Nature* and *Science* detailing a proposed set of experiments that would represent a 'gain of function' on the avian influenza virus H7N9. In contrast to the 2012 incident, the scientists, who would be involved in this research are using these letters to gain early support from government scientific oversight bodies by explaining their risk mitigation plans for the research, and clearly explaining the experiments they wish to complete. Their objective is to make more virulent strains of H7N9 that would spread more easily between people so that they can understand how the virus mutates in nature causing pandemics. The experiments would also increase their understanding about how to develop better early warning surveillance of dangerous strains and better vaccines (Fouchier et al. 2013: 612–613).

All of the examples of 'sensitive' dual use research discussed above and others in Chapter 8 illustrate the potential threats and risks associated with synthetic biology and the manipulation of microbial genetics. The manipulation of naturally occurring viruses like H5N1 or horse pox so they can mutate more easily into hyper virulent variants that are more easily passed from animals to humans, or humans to humans—and the creation of dangerous pathogens using chemically synthesized genomes—show that this kind of knowledge can be put on the radar of interested bio-criminals and terrorists. The rapid advances in biotechnology, or what some describe as the 'industrialization of biology' (Center for Biosecurity of UPMC 2011), can result in faster, cheaper and more effective scientific breakthroughs for health, chemical manufacturing, bio-fuels and mining, but it also highlights a number of other newer threat scenarios for criminal or terrorist exploitation.

There are also concerns amongst biosecurity regulators and national security intelligence agencies that it is not just the *knowledge* that is on offer, but some of the *equipment* and *technology* (used chiefly in the past by scientists working on government funded research projects in BSL-3 and BSL-4 labs), that is becoming more available to the wider public. The increasing growth in biotechnology, the growing accessibility of automated biological techniques and relatively in-expensive equipment (such as that used in DNA sequencing and synthesis), makes scientific experimentation accessible in ways it wasn't even a decade ago to 'citizen scientists' or people interested in DIY ('do it yourself') Bio (Center for Biosecurity of UPMC 2011: 7; Caves and Carus 2014: 27). To illustrate this point, the entire human genome was sequenced in 2003. It took a team of scientists 13 years and nearly half a billion dollars to identify the approximately 20, 5000 genes in humans. In contrast today companies such as *Life Technologies* claim that they can decode a human genome sequence in a day for only $1000 using smaller equipment (such as a benchtop Ion Proton Sequencer) that can be ordered from them (Life Technologies 2012). Other DNA sequences from deadly pathogens can also be bought online. For example, in 2006 a journalist from the Guardian was able to purchase online a short sequence of the small pox DNA (Randerson 2006).

A US National Research Council report, *Globalization, Biosecurity and the Future of the Life Sciences* (NRC 2006), provides a detailed summary of both the global drivers and trajectories of advanced life science technologies that raise biosecurity concerns. There is insufficient room here to provide a comprehensive list of all potential threat and risk scenarios in the biotechnology field and interested readers should consult (NAS 2017; NRC 2006; Tucker 2012: 19–45) for a more detailed understanding of the threat environment. In summary though, the list of potential biotechnological threat scenarios may be endless due to the overlapping skills and technologies involved with synthetic biology. The evolving nature of some biotechnology also prevents a full threat and risk assessment of the security issues that may arise out of such technology.

Additionally, part of the difficulty in trying to assess the boundaries of biotechnological threat scenarios is that in many cases insufficient discussion and analysis has taken place between scientists and their

national security counterparts as to the rationale for assessing an issue as a threat or risk. This is a theme we will return to in Chapters 4, 5 and 7. To provide however, some context of what threats may be possible, Goodman and Hessel (2013) survey a number of scenarios, including what they refer to as: bad bio-technologists, biological spam, phishing for DNA, identity theft, piracy and spear phishing. I will restrict discussion here to three: bad bio technologists, identity theft, and piracy to illustrate how they assess this threat environment might evolve.

The number of biotech companies have expanded at a steady pace over the last decade. For example, US research and development company Battelle in its sixth biennial report on the biosciences industry estimated that in 2012, 1.62 million people were employed across 73,000 individual businesses working across the range of biosciences such as medical and research laboratories, agriculture, and pharmaceuticals (Battelle 2014: v). This does not include the publicly funded biosciences workforce. So Goodman and Hessel argue that based on statistics alone, the sheer increase in people working in biological engineering, there is likely to be a few 'lunatics' with intentions to cause harm. Their analysis is supported by other biosecurity experts, who see that experts with an intent to cause harm or 'bio Unabombers' as more concerning than amateurish bio-hackers in the suburbs (Center for Biosecurity of UPMC 2011: 16; Ellis 2014: 216). While the stockpiles of 'controlled substances such as anthrax may be relatively secure, the DNA code of many of them Goodman and Hessel argue, exists in public data bases, and advances in synthetic biology allows the building of synthetic organisms—thereby sidestepping current safeguards in place for protecting select agents stockpiled in secure sites'.

The second threat scenario Goodman and Hessel describe (identity theft) is a 'new take' on an old enabler of crime. They argue as countries increase their holdings of DNA in national databases for criminal identification, there will be more opportunities for these to be compromised—resulting in people's identities being stolen to enable identity related and other crimes). Additionally, Goodman and Hessel assess in the future a confluence of situations, whereby genetic identity theft could enable people to circumvent health and employment restrictions

based on their genetic data. Genetic cloning or impersonation (leaving another person's DNA at a crime scene) could also frustrate intelligence operations or law enforcement investigations. For example, in 2009, scientists in Israel demonstrated that it was possible to fabricate DNA evidence in a crime scene by fabricating blood and saliva samples containing DNA from a person other than the donor of the blood and saliva (Frumkin et al. 2011: 95–103).

The third interesting threat scenario 'biological piracy' presents a number of security, ethical, policy and legal challenges which remain largely unaddressed. Goodman and Hessel suggest in the future a wide variety of biological and genetic materials will be pirated just like digital media has been. The field of synthetic biology, which is already working towards developing therapies and treatments for cancers and other diseases, provides opportunities for organized crime groups to provide pirated versions (Goodman and Hessel 2013). The recent development in genome editing technology such as Crispr, Finger Nuclease (Zinc) and Talen, which can now manipulate DNA in human germ cells and remove or correct genetic mutations that cause disease might also be manipulated to do the reverse i.e. make people more susceptible to disease or reduce the effect of vaccinations (Corbyn 2015).

Similar to the discussion above of historical and post-9/11 bio-threats, we also need to examine emerging threats by addressing both dimensions of threat assessment—*intention* and *capability*. This is, however, where the challenge begins. The industrialization of biology is happening at such a dynamic and rapid pace, it remains difficult to make reliable estimates of both the future intentions and capabilities of threat actors, who may be interested in exploiting biotechnologies for criminal or terrorist reasons. As one workshop of experts suggested, 'the angles of the attack are almost infinite and very difficult to anticipate' (Center for Biosecurity of UPMC 2012: 15).

Part of the challenge relates to the type of framework used by those in the national security communities and by biosecurity researchers to understand threat and risk. Some frameworks argue for a steady linear increase in biotechnology, and a greater access to skills and technology by bio-criminals and bio-terrorists as a result (Chyba 2006; Carlson 2003; Petro and Carus 2005). In contrast, others have adopted

frameworks that estimate a less linear increase in biotechnology. They argue that mere access to technology and even 'know how' does not automatically create either the motivation or ability for bio-criminals or bio-terrorists to exploit biotechnology for harmful purposes. Adherents to this framework suggest that there is a lot more uncertainty in how biotechnologies may develop in the future, as other non-technological variables such as social, economic, and organizational factors will also influence the growth of technology and the extent to which it is exploited by individuals or groups for nefarious reasons (Vogel 2008).

Careful consideration of how the emerging biosecurity threat context will evolve also needs to include an assessment on whether it is likely that we will see more single actor or group threats, and the consequences for policy makers and first responders. For example, as biotechnological knowledge becomes increasingly commoditized and equipment less expensive, will there be an increase in the rhetoric of well-established international terrorists groups (such as one of the Al Qaeda inspired franchises: al Qaeda in the Arabian Peninsula (AQAP), or al Shabab), declaring an intent to use a virus or bacteria that they have synthesized or acquired via a third party? Alternatively, are we going to see intentions being expressed about the desire to use bio-synthetic agents by less established domestic terrorist groups, or even individuals each with different agendas (jihadists, ultra-nationalists, anarchists/bio-hackers or environmentally motivated individuals)?

As discussed previously, there are very few cases of bio-terror attacks—certainly not enough (thankfully) to make analytical generalizations about the specific motivations of various groups or individuals' desire to weaponise conventional biological agents. It is also doubtful the extent to which extrapolations from these cases will assist estimations about threat actor's intentions to use pathogens produced via for example, synthetic genomics. Some profiling of the intentions and operational decisions made by terrorists and criminals using other medium for attack, however, including cyber may provide guidance on how rhetoric becomes operationalised to use a particular weapon over another. An understanding of cyber facilitated intellectual property theft, for example, may provide insights into how bio-criminals or bio-terrorists may seek to access biotechnology in illegal ways. Perman et al.

(2013: 90–110). We continue this discussion of what other disciplines and fields can teach us about improving our analytical understanding of emerging bio-threats in Chapters 5 and 7. Nonetheless, we need to face the reality that 'getting into the heads' of threat actors, who are not yet on the radar of intelligence and law enforcement agencies remains extremely difficult.

It is difficult enough to assess the intentions of threat actors—some who themselves may not have thought about the attractiveness of biotechnology agents. It seems doubly difficult to assess whether bio-criminals and terrorists will have the capabilities to either access or produce harmful biological agents that have been synthesized in a lab. As difficult, indeed near impossible as it is to assess the future intentions of threat actors as we shall see in Chapters 4 and 5, intelligence analysts and the broader intelligence enterprise do need to make efforts to model intentions behavior for possible bio threats. For example, intentions of potential threat actors could be modeled partially to some extent 'from existing case studies in the biomedical and microbiological field in an effort to establish trends in behavior and tactics' Perman et al. (2013: 91–92). Perman discusses how a National Institute of Justice study that was commissioned to better understand the behavioral indicators in attacks on political leaders resulted in the development of the Exceptional Case Study within the US Secret Service. The Exceptional Case Study is a work in progress in continually refining understanding of adversaries and behavioral indicators that can predict threatening behaviors and risks of violence (ibid.: 92). Perman et al. argues that the results of the Exceptional Case Study are applicable to the life sciences as the same kind of behavioral indicators are in play.

In contrast though to the 'intent' side of the threat equation, some intelligence agencies with mandates to assess the threat and risk of bio-weapons have done a lot more work on estimating the capabilities required by an actor(s) in weaponising various biological agents—including those resulting from genetic engineering or biotechnology. Much of this of course, is classified, but the focus is on the level of expertise and equipment required to operationalise different biotechnological based threat scenarios. Part of this work also relates

to developing better science, technology, particularly microbial forensic analytical skills to detect, and investigate potential bio-criminal and bioterrorism threats (e.g. Murch 2003; Bhattacharjee 2009; Budowle and Williamson 2009; Shea 2006; Inglis et al. 2011). This work seems to be a useful place to start. If agencies continue to have limited visibility on an individuals' intentions (prior to an attack), then re-examining carefully variables related to capability (*knowledge and equipment*), may provide more accurate assessments about the likelihoods of various 'high tech bioterrorism threats' (Suk et al. 2011: 1). If intelligence agencies can develop a more *evidence based* approach to estimating bio-threat capabilities, then they will be in a better place to provide assessments to policy makers, public health, scientists and security managers responsible for developing strategies that mitigate these threats. At the very least, they may be able to provide in some cases more granularity to the analysis of which suite of capabilities may be more vulnerable to exploitation by threat actors than others.

The difficulty however, with working on the capability side of the threat formula (knowledge and equipment) is to, as mentioned earlier, potentially either over or under emphasize both the level of expertise, and margins of difficulty in accessing the equipment required to carry out an attack. For example, some authors recognize the various technical steps required to synthesize a dangerous pathogen, yet argue that these may be less difficult to overcome than it may appear for a 'do it yourself' biologist/terrorist (Burr 2012). However, as discussed previously, knowledge is more than reading a book on synthetic genomics, an actor must also develop the skill base and practical tacit knowledge (trial and error in the scientific process) as well.

In summary, a fixation only on the technologies (and equipment) that various actors could exploit can result in a kind of technical determinism, which blinds intelligence analysis of potential threats—resulting in either an under or over-statement of the threat. There are some in the scientific and biosecurity communities, who may be under-stating the capabilities of future threat actors to use synthetic biology and biotechnology in a bio-attack. For example, during a recent over the horizon scanning project conducted by the US Center for Biosecurity

of UPMC most of the scientists interviewed stated that there exists simple paths for skilled individuals to making bio-weapons that 'render more technically difficult approaches unattractive and therefore less likely to be pursued' (Center for Biosecurity of UPMC 2011: 16). Or as stated in the project teams' report, perhaps in blunter words: 'the bad guys aren't going to waste their time with sophisticated pie in the eye sky stuff' (ibid.). In most cases, assessing actual capabilities will remain challenging and an evidence based approach is needed to avoid 'over' or under-assessing knowledge, equipment and skills. We will come back to the importance of an evidence based approach for assessing emerging bio-threats in Chapter 5.

Conclusion

In this chapter we have surveyed the historical, contemporary and emerging bio-threat landscape to illustrate the complexity of threats and risks that exist. As this survey suggest, understanding the emerging threat environment in particular is very difficult given with many potential threat scenarios there are a number of drivers at play (technology, psycho-social factors, bio-safety and compliance issues and policy) and it remains difficult to determine the effect of these alone and together in enabling certain threat types over time. Does this difficulty mean that those working in the intelligence enterprise cannot provide any understanding on potential bio-threats for decision-makers? The answer has to be clearly no. There are many other different threat types, for example, cyber where it is difficult to interpret what might be the key emerging threats, but decision-makers still need support in understanding, preventing, disrupting or reducing such threats to the extent that they can be understood.

Intelligence agencies cannot simply say to decision makers 'sorry it's too hard' as this would not be a recipe for continued funding. So the question now to be explored in the next three chapters is given this uncertain and complex bio-threat environment, what role should

intelligence play, how has the role of intelligence changed since 9/11 and what challenges and opportunities are there for biosecurity intelligence practice? Chapter 3 will begin to address these questions by exploring how intelligence might be tasked by decision-makers interested in understanding bio-threats and risks and what challenges and opportunities exist for improving each 'Five Eyes' country's response to complex and uncertain bio-threats and risks?

Notes

1. These agents are referred to as 'Category A' bio agents (denoted as such because they have the greatest capacity for harm if used in a bioterrorist attack). The reader should refer to either the World Health Organization (WHO) or the US Center for Disease Control (CDC) websites for good overviews of these agents and others on the Category A list such as small pox, viral hemorrhagic fevers and botulism.
2. SARS or severe acute respiratory syndrome is a corona virus originally sourced to China's Guangdong province. It causes severe life threatening pneumonia. It is highly contagious and the 2003 outbreak resulted in the deaths of 8000 people globally. HINI virus results in a highly contagious flu for humans. It is closely related to a number of animal influenza sources. Early outbreaks started in North America and by June 2009, the WHO declared it a pandemic after the virus spread globally-killing over 16,000 people.
3. Global investment company, Morgan Stanley, predicted in 2003 that the SARs virus would shave more than $15 billion off the output of Asian economies; while the WHO predicted that the global cost could be more than $30 billion. See Watts and Stewart (2003).
4. The National Academies committee produced a report in 2004 called, 'Biotechnology Research in an Age of Terrorism' (sometimes also referred to as the 'Fink Report). The Report contained seven recommendations to ensure responsible oversight for biotechnology research with potential bioterrorism applications. One of these was to create a National Science Advisory Board for Biodefense to provide advice, guidance, and leadership for a system of review and oversight of experiments of concern.

References

Alibek, K. (1999). *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World—Told from the Inside by the Man Who Ran It*. New York: Random House.

Balmer, B. (2001). *Britain and Biological Warfare. Expert Advice and Science Policy, 1930–65*. Basingstoke, UK: Palgrave Macmillan.

Battelle. (2014). *Battelle/Bio State Bioscience, Jobs, Investments and Innovation*. Columbus, OH: Battelle.

Bhattacharjee, Y. (2009). News of the Week. Paul Keim on His Life with the FBI During the Amerithrax Investigation. *American Association for the Advancement of Science, 323*, 1416.

Bombardt, J. (2000). *Contagious Disease Dynamics for Biological Warfare and Bioterrorism Casualty Assessments*. Alexandria, VA: US Department of Defense.

Bravata, D., et al. (2004). Systematic Review: Surveillance Systems for Early Detection of Bioterrorism Related Diseases. *Annals of Internal Medicine, 40*(11), 910–924.

Budowle, B., & Williamson, P. C. (2009). *Microbial Forensics Wiley Encyclopaedia of Forensic Science.* John Wiley & Sons, Ltd.

Burchill, S., et al. (Eds.). (1996). *Theories of International Relations*. Basingstoke, UK: Palgrave Macmillan.

Burnette, R. (Ed.). (2013). *Biosecurity Understanding, Assessing, and Preventing the Threat*. Hoboken, NJ: Wiley.

Burns, R. (2015). US Military Says It Mistakenly Shipped Live Anthrax Samples. From http://www.nbcnewyork.com/news/national-international/Pentagon-Shipped-Live-Anthrax-Samples–305221031.html. Accessed March 13, 2017.

Burr, J. (2012). The Mad (and Not So Mad) Scientist Next Door: A Holistic Approach to Addressing Do-it-Yourself Biology. *Journal of Biosecurity, Biosafety and Biodefense Law, 3*(1), ISSN (Online) 2154–3186. https://doi.org/10.1515/2154-3186.1035.

Carlson, R. (2003). The Pace and Proliferation of Biological Technologies. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, 1*(3), 203–214. https://doi.org/10.1089/153871303769201851.

Carus, S. (2001). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*. Washington, DC: National Defense University.

Carus, S. (2017). Occasional Paper 12. A Short History of Biological Warfare: From Pre-history to the Twenty-First Century. *Center for the Study of Weapons of Mass Destruction*. Washington, DC: National Defense University.

Cass, S. (1999). Researcher Charged with Data Theft. *Nature Medicine, 5*, 474. https://doi.org/10.1038/8350.

Caves, J., & Carus, W. (2014). The Future of Weapons of Mass Destruction: Their Nature and Role in 2030 (Occasional Paper No 10, pp. 1–75). *Center for the Study of Weapons of Mass Destruction*. Washington, DC: National Defense University.

Center for Biosecurity of UPMC. (2011). Center for Biosecurity. US Government Judgments on the Threat of Biological Weapons: Official Assessments, 2004–2011 (pp. 1–26). Baltimore, MD: Center for Biosecurity of UPMC.

Center for Biosecurity of UPMC. (2012). *The Industrialization of Biology and its Impact on National Security*. Baltimore, MD: Center for Biosecurity of UPMC.

Christopher, G., et al. (1997). Biological Warfare: A Historical Perspective. *Journal of the American Medical Association, 278*(5), 412–417.

Chyba, C. (2006). Biotechnology and the Challenge to Arms Control. *Arms Control Today, 36*, 11–17.

Corbyn, Z. (2015, 10 May). *Crispr: Is It a Good Idea to Upgrade? The Observer*. Retrieved from http://newsrule.com/crispr-is-it-a-good-idea-to-upgrade-our-dna/.

Crawford, D. (2007). *Deadly Companions*. Oxford: Oxford University Press.

DOJ. (2010). *The United States Department of Justice. Amerithrax Investigative Summary*. Washington, DC.

Edge, J., & Hoffman, S. (2015). Strengthening National Health Systems Capacity to Respond to Future Global Pandemics. In S. Davies & J. Youde (Eds.), *The Politics of Surveillance and the Response to Disease Outbreaks* (pp. 157–179). Surrey, UK: Ashgate.

Elliott, S. (2007). The Threat from Within: Trade Secret Theft by Employees. *Nature Biotechnology, 25*(3), 293–295. https://doi.org/10.1038/nbt0307-293.

Ellis, P. D. (2014). Lone Wolf Terrorism and Weapons of Mass Destruction: An Examination of Capabilities and Countermeasures. *Terrorism and Political Violence, 26*(1), 211–225. https://doi.org/10.1080/09546553.2014.849935.

Fouchier, R., et al. (2013). Gain-of-Function Experiments on H7N9. *Science*. https://doi.org/10.1126/science.1243325.

Friedman, D. (2015). Towards WMDFZ in the Middle East: Biological Confidence Building Measures. In H. Muller & D. Muller (Eds.), *WMD Arms Control in the Middle East. Prospects, Obstacles and Options* (pp. 176–180). Farnham, UK: Ashgate.

Frumkin, D., Wasserstrom, A., Budowle, B., & Davidson, A. (2011). DNA Methylation-based Forensic Tissue Identification. *Forensic Science International: Genetics, 5*(5), 517–524. http://dx.doi.org/10.1016/j.fsigen.2010.12.001.

GAO. (2013). High Containment Laboratories: Assessment of the Nation's Need Is Missing. *Testimony Before The Subcommittee Emergency Preparedness, Response and Communications, Biosurveillance Observations on the Cancellation of Biowatch Gen-3 and Future Considerations for the Program*, 18 (2014).

Geissler, E., & van Courtland Moon, J. E. (Eds.). (1999). *Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945*. New York: Oxford University Press.

Goodman, M., & Hessel, A. (2013). The Bio-crime Prophecy: DNA Hacking the Biggest Opportunity since Cyber Attacks. *Wired*. From http://www.wired.co.uk/article/the-bio-crime-prophecy. Accessed March 14, 2017.

Gronvall, G. (2012). *Preparing for Bioterrorism*. Baltimore, MD: Center for Biosecurity of UPMC.

Inglis, T., et al. (2011). Forensic Investigation of Biological Weapons Use. In J. Gall & J. Payne-James (Eds.), *Current Practices in Forensic Medicine* (pp. 17–42). Chichester, UK: Wiley.

Koblentz, G. (2009). *Living Weapons*. New York: Cornell University Press.

Lucero, C., et al. (2011). Biosurveillance Applications. *BMC Medical Informatics, 11,* 1–12.

Leitenberg, M. (1999). Aum Shinrikyo's Efforts to Produce Biological Weapons: A Case Study in the Serial Propagation of Misinformation. *Terrorism and Political Violence, 11*(4), 149–158. https://doi.org/10.1080/09546559908427537.

Leitenberg, M. (2005). *Assessing the Biological Weapons and Bioterrorism Threat*. Carlisle, PA: Strategic Studies Institute of the US, Army War College.

Life Technologies. (2012, 10 January). *Life Technologies Introduces the Benchtop Ion ProtonTM Sequencer; Designed to Decode a Human Life Genome in One Day for $1,000*. Press release at http://www.lifetechnologies.com/content/lifetech/us/en/home/about-us/news-gallery/press-releases/2012/life-techologies-itroduces-the-bechtop-io-proto.html.

Maher, B. (2012). The Biosecurity Oversight. *Nature, 485*, 431–434.
May, L., et al. (2009). Beyond Traditional Surveillance: Applying Syndromic Surveillance to Developing Settings—Opportunities and Challenges. *BMC Public Health, 9*(1), 242. https://doi.org/10.1186/1471-2458-9-242.
McLeish, C., & Nightingale, P. (2007). Biosecurity, Bioterrorism and the Governance of Science: The Increasing Convergence of Science and Security Policy. *Research Policy, 36*(10), 1635–1654. https://doi.org/10.1016/j.respol.2007.10.003.
McNeil, W. (1998). *Plagues and Peoples*. New York: Anchor Books.
Mearsheimer, J. (2001). *The Tragedy of Great Global Power Politics*. New York: Norton.
Morgenthau, H. (1967). *Politics Among Nations* (4th ed.). New York: Knopf.
Murch, R. (2003). Microbial Forensics: Building a National Capacity to Investigate Bioterrorism. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, 1*(2), 1–5.
NAS. (2017). *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology: Interim Report*. Washington, DC: National Academy of Sciences.
Neville, S. (2013, May 28). Horsemeat Lasagne Scandal Leaves Findus Reputation in Tatters. *The Guardian*. From https://www.theguardian.com/business/2013/feb/08/horsemeat-lasagne-scandal-findus-reputation. Accessed March 15, 2017.
Nicolaides, C., et al. (2012). A Metric of Influential Spreading During Contagion Dynamics Through the Air Transportation Network. *PLOS One, 7*(7), 1–10.
NRC. (2004). *Biotechnology Research in an Age of Terrorism*. Washington, DC: National Academies.
NRC. (2006). *Globalization, Biosecurity and the Future of the Life Sciences*. Washington, DC: Institute of Medicine and National Research Council.
Perman, B., et al. (2013). Basic Principles of Threat Assessment. In R. Burnette (Ed.), *Biosecurity: Understanding, Assessing, and Preventing the Threat* (pp. 89–90). Hoboken, NJ: Wiley.
Petro, J., & Carus, S. (2005). Biological Threat Characterisation Research: A Critical Component of National Biodefense, Biosecurity, and Bioterrorism. *Biodefense Strategy, Practice and Science, 3,* 295–308.
Pita, R., & Gunaratna, R. (2009). Revisiting Al-Qaeda's Anthrax Program. *CTC Sentinel, 2*(5), 10–13.
Randerson, J. (2006, May 28). Revealed: The Lax Laws that Could Allow the Assembly of Deadly Virus DNA. *The Guardian*. From https://www.theguardian.com/world/2006/jun/14/terrorism.topstories3. Accessed March 15, 2017.

Regis, E. (1999). *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company.
Rosenau, W. (2001). Aum Shinrikyo's Biological Weapons Program: Why Did It Fail? *Studies in Conflict and Terrorism, 24,* 283–301.
Salama, S., & Hansell, L. (2005). Does Intent Equal Capability? Al Qaeda and Weapons of Mass Destruction. *Nonproliferation Review, 12*(3), 615–653.
Salerno, R. (2015). Three Recent Case Studies: The Role of Biorisk Management. In R. Salerno, J. Gaudioso, (Eds.), *Laboratory Biorisk Management. Biosafety and Biosecurity* (pp. 191–202). Boca Raton, FL: CRC Press.
Schnirring, L. (2014, August 15). CDC Probe of H5N1 Cross Contamination Reveals Protocol Lapses, Reporting Delays. *CIDRAP*. From http://www.cidrap.umn.edu/news-perspective/2014/08/cdc-probe-h5n1-cross-contamination-reveals-protocol-lapses-reporting-delays. Accessed March 15, 2017.
Shea, D. (2006). The National Biodefense Analysis and Countermeasure Center: Issues for Congress *CRS Report* (Vol. RL32891). Washington, DC: Congressional Research Service, The Library of Congress.
Silberman, L., & Robb, C. (2005). *Commission on the Intelligence Capabilities of the US Regarding Weapons of Mass Destruction. Report to the President of the United States* (pp. 1–501). Washington, DC.
Spiers, E. (2010). *A History of Chemical and Biological Weapons*. London: Reaktion Books.
Stattner, E., et al. (2011). Diffusion in Dynamic Social Networks: Application in Epidemiology. In A. Hameurlain et al. (Eds.), *Database and Expert Systems Applications* (pp. 559–573). Heidelberg: Springer-Verlag GMBH.
Suk, J., et al. (2011). Dual Use Research and Technological Diffusion. Reconsidering the Bioterrorism Threat Spectrum. *PLOS Pathogens, 7*(1), 1–3.
Tenet, G. (2007). *At the Center of the Storm: My Years at the CIA*. New York: HarperCollins.
Trevett, C. (2013, May 28). Fonterra Chief Gets 'Frank and Thorough Grilling'. *New Zealand Herald*.
Tucker, J. (Ed.). (2012). *Innovation, Dual Use and Security*. Cambridge, MA: The MIT Press.
Tumpey, T. M., et al. (2005). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science, 310*(5745), 77–80. https://doi.org/10.1126/science.1119392.
UNMOVIC. (2007). Compendium of Iraq's Prescribed Weapons Programmes in the Chemical, Biological and Missile Areas (pp. 765–1030). New York, UN.
US Army. (2008). *Army Regulation 50–1. Biological Surety*. Washington, DC: US Department of Defense.

Vogel, K. (2008). Biodefense. In A. Lakoff (Eds.), *Biosecurity Interventions* (pp. 227–255). New York: Columbia University.

Walsh, P. F. (2011). *Intelligence and Intelligence Analysis*. Abingdon, UK: Routledge.

Walsh, P. F. (2014). Managing Intelligence and Responding to Emerging Threats: The Case of Biosecurity. In M. Gill (Ed.), *The Handbook of Security* (pp. 837–854). Basingstoke: Palgrave Macmillan.

Waltz, K. (1979). *Theory of International Politics*. New York: Random House.

Watts, J., & Stewart, H. (2003, April 22). Asia Unable to Mask SARS Cost. *The Guardian*.

Wein, L., & Liu, Y. (2005). Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk. *Proceedings of the National Academy of Sciences of the United States of America, 102*(28), 9984–9989. https://doi.org/10.1073/pnas.0408526102.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Williams-Jones, B., Olivier, C., & Smith, E. (2014). Governing 'Dual-Use' Research in Canada: A Policy Review. *Science and Public Policy, 41*(1), 76–93. https://doi.org/10.1093/scipol/sct038.

Yam, A. (2013, May 28). Memories Still Too Raw for Chinese Parents to Trust Baby Formula. *South China Morning Post*. From http://www.scmp.com/news/china/article/1273375/memories-still-too-raw-chinese-parents-trust-baby-formula. Accessed March 15.

Zanders, J. (2015). Biological and Chemical Weapons and the Prospective Disarmament Process in the Middle East. In H. Muller (Eds.), *WMD Arms Control in the Middle East* (pp. 149–157). Surrey, UK: Ashgate.