3

Intelligence Tasking and Coordination

Biosecurity and Intelligence

In this chapter, we move our attention away from an assessment of the biosecurity environment to a detailed analysis of the core intelligence processes (tasking and coordination, collection, and analysis). In other words, Chapters 3–5 examine what role intelligence should play in responding to the emerging threats discussed in Chapter 2. In the biosecurity context, as in any other, intelligence is a 'service industry' whose sole aim ought to be to interpret the threat and risk environment for a decision-maker in order that they can either disrupt threats or put in place mitigation strategies. Put another way, national security intelligence and law enforcement agencies play a role both in reducing uncertainty around the biosecurity environment, and the impact of threats and risks associated with it. The degree to which intelligence can interpret emerging bio-threats will depend on the issue, and the extent to which intelligence agencies are able to provide 'value added' information in a timely manner for decision-makers. On this point, history shows that intelligence agencies have had a mixed record in assessing bio-threats accurately

P. F. Walsh, *Intelligence, Biosecurity and Bioterrorism*,
https://doi.org/10.1057/978-1-137-51700-5_3

during the Cold War, and perhaps most spectacularly on the extent to which Iraq still had a bio-weapons program in 2003 prior to the second Gulf War (Koblentz 2009: 141–199; Vogel 2013).

The dynamic, evolving and dual use nature of emerging bio-threats, present multiple collection and analytical challenges for intelligence agencies. While it may be possible to track some steps along a planned attack, for example, irregular financial transactions, or detecting a series of suspicious supply orders for equipment—it may be even more difficult (despite advances in microbial forensics) to link this to an individual or groups. The choice of biological weapon may also be an agent that agencies have never 'red teamed' previously with fewer predicate operational steps. It may not be the 'classical anthrax attack' that has defined much of the Cold War and early post-Cold War period threat perception. The bio-attack could be as simple as the planned, systematic food poisoning of multiple trans-Atlantic flights over a one week period. If the terrorist group or individual has never been under surveillance; collection and analytical efforts may only lead to their 'footprints' in the best case just prior or worse after the attack.

Such a complex threat and risk environment provides multiple challenges for decision-makers in how they task intelligence agencies and communities effectively. The rapid advances in the biological sciences and biotechnology as discussed in Chapter 2 suggest that particularly at the strategic end, but also at the tactical and operational levels decision-makers are not necessarily the most well equipped to task our intelligence communities on what bio-threats and risks they most want to know about. Similarly, the pace in the advances of biological sciences that could be potentially 'weaponised' or 'criminalised' also challenge both the intelligence and scientific communities' ability to fully keep pace with how potential threats and risks may develop during the next decade. Despite the innate difficulties in decision-makers and intelligence communities understanding where potential bio-threats and risks will occur, the intelligence production process does require some focus, which in turn means decisions need to be made about where limited collection and analytical resources will be applied. This means that the political leadership and intelligence communities themselves need to delineate specific tasking areas for further action. This chapter will draw on a combination of

interviews of senior intelligence officers and secondary sources to identify, to the extent that this is possible, what decision-makers across the 'Five Eyes' intelligence communities are saying are their biosecurity tasking priorities and how are the coordinated. There can be no effective tasking without specific requirements being coordinated across the tasked agency or community so our tasking discussion below will also include how the political leadership tasks are coordinated across 'Five Eyes' intelligence communities. Are coordination efforts optimal and if not where do the challenges remain and what can be done about them?

While much of the specifics of actual tasking requirements are classified, it is possible to gain a broad overview (rather than an exhaustive list) of some priority tasking areas. A sample of tasking requirements will be discussed at their strategic, operational and tactical levels to illustrate how in reality tasking at one level (for example strategic) has tasking implications at other levels of decision-making (operational and tactical). And as mentioned earlier, political leaders cannot be expected to understand fully the complex suite of biosecurity threat and risk trajectories that may unfold over the next decade. Hence, intelligence communities themselves, as they have often done in the past will need to 'manage upwards' to help political decision-makers identify and make better tasking decisions. The chapter, will therefore, examine how in some 'Five Eye's' settings intelligence agencies and communities manage up to alert their political leadership on the nature of both actual and potential biosecurity threats. The third objective of this chapter is to examine what role the intelligence communities' understanding of concepts of bio-threat and bio-risk play in the tasking of intelligence; and whether risk and threat assessment methodologies are sufficiently effective in steering tasking and coordination efforts.

Biosecurity Intelligence Tasking Priorities

As noted in Chapter 2, the biosecurity threat and risk spectrum is diverse and difficult to pin down given the pace at which advancements in the biological sciences and uptake of technology is taking place. Each of the 'Five Eyes' countries has a national intelligence priority setting

process set by the executive branch of government, which broadly outlines the key national security issues that the government considers priorities for guiding its prosecution of national security policy making. This 'list' of national intelligence priorities provides the bare bones of what the national political leadership needs to know about and it then becomes the responsibility of the intelligence community to both collect and assess a range of sensitive and open source information in a way that services those priorities. National intelligence priorities are a statement of what the nation's executive consumers of intelligence are most interested in the intelligence community spending collection and analytical resources on.

In the United States, the priorities list is called the National Intelligence Priorities Framework and is signed off by the President in consultation with the national security principal's committee. The principals being senior administration officials such as the Secretaries of Defence and State amongst others. Although the National Intelligence Priorities Framework could be seen as a top down driven process, it also completed in coordination with advice from officials within the National Intelligence Council (NIC). The NIC is controlled by the Office of the Director, National Intelligence. It is made up of national intelligence officers and is primarily responsible for producing national intelligence estimates on emerging or complex issues.

Similarly in Australia, Canada and the UK, a centralized national security priority setting process exists. In the case of Australia, the National Intelligence Priorities are set by the highest national security policy making body of the Government—the National Security Committee of Cabinet. While in the US, the ODNI has the responsibility to ensure that collection and analytical activities across the intelligence community are meeting priorities set in the framework, in Australia it is the responsibility of high level committees (e.g. the National Intelligence Coordination Committee and the National Intelligence Collection Management Committee) within the Department of Prime Minister and Cabinet to ensure collection and assessment priorities as set out in the national intelligence priorities are being addressed by the Australian intelligence community. At the time of writing however, changes are underway in the coordination of

Australia's intelligence community with the creation of a new Office of National Intelligence which may alter some of the mechanisms in how intelligence priorities are set and coordinated.

Similarly in the US since 9/11, and to some extent in the other 'Five Eyes' countries there have been a series of 'flag ship' policy declarations on biosecurity and bio-terrorism, which have also provided specific guidance and recommendations to intelligence communities on how to improve their capabilities in dealing with biosecurity threats and risks. Other policy statements have sought to provide broader strategic guidance to communities. Some of these have been executive policy initiatives, while others have been parliamentary or special reviews by legislators, which have provided specific recommendations for improving the intelligence response to bio-threats and risks. For example, the Silberman and Robb Commission Report to the Bush Administration in response to the failures of the intelligence community's prewar judgements on Iraq's WMD capability and concern over *Amerithrax* devoted an entire chapter (Chapter 13) that dealt with how tasking, coordination, collection and analysis of bio-threats and risks could be improved across the intelligence community (Silberman and Robb 2005). More recently other policy declarations such as the Obama Administration's 2009 *National Strategy for Countering Biological Threats* provided the US intelligence community broad strategic guidance on the role the intelligence community could play, along with other public health and international cooperation strategies in the prevention of 'bio-attacks' (both natural pandemics and those caused by threat actors).

Understanding, how intelligence agencies have been tasked on both the collection and analysis of bio-threats and risks since 9/11, therefore, also requires knowledge of what policy initiatives 'Five Eyes' governments have implemented to improve intelligence decision-making support across the evolving bio-threat and risks spectrum.

The national intelligence priorities setting frameworks of all 'Five Eyes' countries use an alpha or numeric category system to denote which priorities decision-makers want the intelligence communities to collect and assess more on. While there is a potentially endless and diverse range of threats and risks (e.g. terrorism, cyber, organized crime and state based threats), resources are limited as is the attention span

of the political leadership to deal with all issues as equal priorities. The US National Intelligence Priorities Framework uses a matrix, which rates the highest priorities and interest to the leadership as Tier 1 and the lowest as Tier 5. The US framework also links intelligence issues to specific geographic targets, organisations and issues. All national intelligence priority setting frameworks across the 'Five Eyes' are classified for obvious reasons, though various public policy declarations on national security issued by their governments make it reasonably clear what the relative priority of certain issues would be on their classified lists (see for example, DNI Clapper's 2016 World Wide Threat Assessment, Australia's 2015 Counter-Terrorism Strategy or national cyber strategies in each 'Five Eyes' country).

It is clear for example in Washington DC, London, Ottawa, Wellington and Canberra that governments are concerned with state based threats such as: China's role in the twenty-first century, North Korea's WMD proliferation, the resurgence of Russia, and instability in Pakistan, Afghanistan, Syria, Iraq and Libya. It is also clear that leaders are concerned with non-state actor issues, particularly terrorism and issues, which can be either enabled or exploited by state and non-state actors such as cyber-attacks. Priority frameworks also include broad guidance on what issues under each subject decision-makers are particularly interested in. So for China or North Korea, there would be interest in leadership dynamics in these countries and how they impact on national security announcements and actions by the leadership. Since the Cold War to the present, the broad subject area of weapons of mass destruction (WMD) have long been of top priority for 'Five Eyes' countries. As noted in Chapter 2, state based industrial biological weapons programs of the former Soviet Union during the Cold War and other more modest programs of rogue countries (during a similar time frame 1945–1990) such as Iraq, Libya, Iran, North Korea, Rhodesia and South Africa demonstrate that biological weapons capable of mass destruction were a top intelligence collection and analytical priority. Though the other categories of WMD—nuclear and chemical have traditionally been given more collection and analytical attention. And in the current post 9/11 environment, biological aspects of WMD are seen by many in the 'Five Eyes' intelligence communities as 'the

poor man's cousins' in terms of collection and analytical priority. This is partly, as noted in Chapter 1, because monitoring nuclear proliferation from an intelligence perspective is easier than assessing whether dual use biotechnology is being weaponized, and also due to except in a few circumstances (*Amerithrax*, Iraq's WMD)—decision-maker's interest in biological weapons has not been consistently high over successive governments across the 'Five Eyes'.

Indeed it is true that from the Bush Administration's early post 9/11 focus on *Amerithrax* and the potential that either terrorists or Iraq would use biological weapons, 'classical bio' (WMD) became a top intelligence priority for the US intelligence community. As Koblentz notes in particular the intelligence support was critical to a range of biodefense programs the Bush Administration initiated. However, since the Bush Administration the priority given to intelligence support for classical bio (WMD) seems to have reduced. If one looks at the Obama Administration's 2010 National Security Strategy, it made clear that 'the spread of nuclear weapons is a top priority' and nearly 1 and a half pages were devoted to it compared to one paragraph on biological weapons (Obama 2010). While President Obama's renewed focus on global health security is also mentioned towards the end of the document, there is no discussion about the criticality of the role of intelligence in working with other important stakeholders such as public health officials or the scientific community. A year after the West Africa Ebola epidemic erupted, President Obama's 2015 National Security Strategy—focused a lot more on improving the global health security agenda to manage health security threats—particularly through capacity building for prevention and detection. Though again there was no mention specifically of the role of intelligence in this greater emphasis on pandemics and infectious diseases. Like the 2010 statement, the 2015 version also detailed the high priority the Administration placed in containing nuclear and chemical proliferation. Concern about biological weapons is reduced to the inclusion of just two words 'biological weapons' towards the end of section on WMD issues (p. 11). It does seem that the nuclear and increasingly the chemical proliferation dimensions of WMD (particularly since finding chemical weapons in Libya (2014) and Syria in (2013) and more recently) were more a focus for senior officials in the

Obama Administration. Other potential non-WMD bio-threats or risks, with the exception of more recent concerns raised in 2016 about the gene editing tool CRISPR also don't seem to be grasping the attention of the leadership of 'Five Eyes' countries. One US senior official said in a discussion with me in 2016 that 'we should be doing more on this (bio-threats and risks) but it's difficult and there are multiple other challenges' (terrorism, cyber, China and Russia). Another senior US official also indicated that non-WMD bio-threats and risks (presumably including potential threats from dual-use biology) would be at the lowest priority level of the intelligence framework, i.e. Tier 5 if they appear at all.

It would be wrong to suggest that a reduction in the number of paragraphs allocated to discussing bio-threats and risks in public versions of flagship policy documents such as National Security Statements means the Obama Administration did not see these issues as no longer intelligence priorities. Indeed my discussions in the US with key senior intelligence staff, who have been engaged in biosecurity threat and risk issues from the Bush and Obama Administrations suggest that bio-threats and risks are still priority issues for the intelligence community. Though some of these same intelligence staff implied that the US did not view bio-threats and risks at the same level as other threats such as 'conventional (non WMD) terrorism', cyber or North Korea.

However, it is clear if one examines both the Bush and Obama's Administration's biosecurity policy making that how bio-threats and risks were perceived and the priority placed on them has changed since 9/11—thereby impacting on the way the US intelligence community was tasked on these issues. As Koblentz notes, the Bush Administration's bio-defense policy making was primarily engaged in defending against domestic threats posed by disease outbreaks caused by terrorists and state actors. Koblentz suggest that 'up to 40 percent (or $23.6 billion) spent on biodefense (from 2001 to 2009) was for research and development of counter measures, diagnostics and sensors and the construction of high containment labs' (2012: 136–137).

As we shall see in the following two chapters (Chapters 4 and 5), various US intelligence agencies had a role in helping develop support for such bio-defense measures including the FBI and DHS. The bio-defense focus of the Bush Administration also of course included the ability of

the DOD to improve its warfare detection of biological weapons, but under the Bush Administration global health and bio-defense issues were kept separate which impacted (particularly early in the Administration) on the way the intelligence community was tasked and how it worked with the public health agencies also working on bio-risks and threats. One senior US official working in the biosecurity area did suggest to me, however that although the Bush Administration was focused on bio-defense, by the mid 2005s the pendulum started to swing back to public health issues that may not be caused by states or terrorists. This evolving focus by the Bush Administration on a global health agenda became a prelude to arguably an even larger focus on global health by the Obama Administration. Though as the pendulum started moving away from bio-defense it became unclear what coherent role the US intelligence community would play in global health and preventive measures against pandemics.

The Obama Administration while continuing many of the bio-defense measures introduced by President Bush shifted the focus to prevention (i.e. laboratory bio-safety, export controls and biological threat reduction programs overseas) (Koblentz 2012: 136–137). The policy interest was also more on a one health approach, and the need to develop global health security measures—not just domestic ones to prevent, detect and rapidly respond to increasing biological threats like Ebola and Zika.

It is clear from the above discussion that intelligence priority setting or tasking of the 'Five Eyes' intelligence communities has changed since 9/11 as the perceived bio-risks threats and interests of decision-makers evolve. Additionally, while biosecurity intelligence tasking as noted earlier, is officially set at the cabinet level of each 'Five Eyes country', tasking regularly occurs at principal's level (ministers or in the case of the US secretary level), deputy-principal level (sub-cabinet level), head of agency and then at lower levels within a range of agencies (both intelligence and non-intelligence) that have some remit for managing bio-threats and risks. The US with 17 agencies has the largest intelligence community, while New Zealand is at the other end of the scale with just three core agencies officially included. The scale and number of intelligence agencies therefore will impact on both how government set intelligence priorities in the biosecurity area and how they are operationalized.

In addition, and as discussed further in Chapters 4 and 5, different member agencies of each country's intelligence communities have distinct functions. Some like the CIA have a foreign intelligence focus, while others such as the Australian Security Intelligence Organisation (ASIO) are more focused on domestic security intelligence collection. Some agencies such as the National Security Agency (NSA) (in the US) or the Government Communications Headquarters Communication (GCHQ) (in the UK) have a collection remit—while others such as the Office of National Assessments (Australia) and the National Assessments Bureau (New Zealand) have an all source assessment responsibility. Similarly some agencies have a hybrid collection and assessment responsibility, particularly agencies such as ASIO, the Canadian Security Intelligence Service (CSIS) or MI5. Further away from the traditional 'inner circle' of traditional intelligence agencies others such as national law enforcement/investigations agencies such as: the Australian Federal Police (AFP), the FBI or the Royal Canadian Mounted Police (RCMP) have both a collection, assessment and prosecution function.

Even further afield from the national intelligence communities of 'Five Eyes' countries there are agencies, which may have some collection and analytical roles in managing bio-risks and threats; including but not limited to: immigration/customs/border protection, agriculture and food safety, public health and animal health authorities.

The potentially large number of government agencies involved in the collection and assessment of bio-threats and risks across each 'Five Eyes' country makes it difficult to take an accurate snapshot in time on how each agency would be involved in managing such threats; including how they would be tasked on these or task others. The tasking processes involved in all cases will be different from agency to agency—depending on the priority that an agency ascribes to supporting any national intelligence effort against a bio-threat or risk. The kind of tasking would as indicated above also be contingent on what unique collection or analytical assets the agency could bring to understand a current or emerging bio-threat/risk. For example, in a sudden yet suspicious disease outbreak tasking a national public health authority with the appropriate epidemiological intelligence staff to collect relevant

data along with an investigatory agency such as the FBI might well be more appropriate then deploying less useful intelligence assets (at least initially) such as sigint collection.

It is not possible therefore to clearly delineate in every case how intelligence is being tasked by decision-makers to arrive at a complete picture of current or emerging bio-threats and risks priorities. It is equally not possible to describe with accuracy in every circumstance which decision-makers are doing the tasking. In reality, although national intelligence communities are tasked with priorities to work on, the tasking process tends to be more dynamic, fluid and even adhoc. Bio-threats and risks can change in real-time and they are of course more difficult to assess the further they are away from the present. In these respects, they are no different from any other threats and risks (e.g. terrorism, cyber, organized crime, WMD, state based threats) in the security environment. For example, we have seen how the threat from Islamic terrorism has evolved and splintered into various new groups and manifestations from Al Qaeda central to Al Shabab (East Africa), Al Qaeda in the Islamic Maghreb (North West Africa) to Islamic State (in Syria and Iraq) and the growth in lone actor (wolf) attacks in the West.

Additionally, since 9/11 there has been a greater blurring across the old lines of domestic and, foreign threats. This has been particularly been the case with transnational threats such as terrorism, drug trafficking and arms trading. Globalisation and the fast pace changes in digital communications have created a more fluid threat and risk space. Al Qaeda and IS may have international dimensions yet the threat and risk posed by them is also regional, national and even local if one thinks about how they (particularly the latter) have inspired lone actor attacks in the last decade.

If such threats are manifesting themselves at different yet inter-connected dimensions (transnational, regional, national and local), intelligence tasking has since 9/11 also become more clearly focused at dealing with threats at these different levels.

Despite the inherent challenges identified above in understanding how intelligence tasking is being done in the dynamic post 9/11 security environment, it is nonetheless possible to gain some insights into tasking and coordination processes. All intelligence tasking is influenced by

two major factors: the time frame required in which a decision needs to be made and the kind of decision that needs to be made. Time frames for decision-making will always be government, community or agency dependent. For example, the military may require intelligence on potential new bio-threats from dual-use technology that they might need to prepare vaccines against over the next 5–10 years. In contrast, a suspicious white powder left on the subway in a major city will likely require intelligence support almost immediately from a city police force. Both situations will involve decision-makers seeking different kinds of intelligence support. Tasking of intelligence therefore happens in different time periods and involves different levels of decision-makers. So while it is difficult to discern exactly in every case 'who', 'by', and 'how' intelligence is tasked it's clear that tasking occurs at the strategic, operational and tactical levels.

Strategic tasking is normally thought of as that which has an 'emerging' or 'over the horizon' focus. Operational tasking is normally, weeks or a year—while a tactical focus is usually the present or out to about a week. These are rough timeframes and as noted above, the actual time frames denoted for each decision-making category are dependent on the threat/risk context and the agencies involved. The development of a threat over a year could, in some agencies, be considered a strategic tasking matter, while in the military this may be considered an operational threat space.

In our scenario of a suspicious white powder being left at three subway stations scenario tasking at the tactical, operational and strategic level might look quite different. At the tactical level, local law enforcement and other first responders (fire department/HAZMAT) would immediately respond to the incident. Immediately on the ground police commanders will be wanting to collect intelligence from any surveillance tapes and start interviewing witnesses. It would be unusual if the discovery of white powder across each site (subway station) would be found and reported to police at the exact same time; so initial tactical intelligence may not immediately show the significance of one incident or how it is connected to the other two. As further information is available,

public health officials and national law enforcement agencies with specialized investigative capabilities would become involved and the depth and breadth of intelligence available and required to support this kind of investigation would be more detailed and service a broader range of decision-makers—including the local and state governments and likely at this stage the national government. Later the same day, bio-forensic testing of the substance may confirm that the powder is live Anthrax and the investigation would now become even broader and rely on the collection and assessment of intelligence further afield from the incident site.

At some stage, a witness statement and the forensic analysis of the substance may provide further information on person(s) of interest. Again a wider number of agencies across the intelligence community would then collect and assess further intelligence on the persons of interest to assess their identity, motivations and capabilities. Foreign intelligence collection assets (sigint, humint) and liaison with other 'Five Eyes' partners may also be tasked to assess if the persons of interest were working domestically or if there was international dimensions to the threat. Let's say in our hypothetical scenario, the investigation concludes a lone-actor terrorist is involved. Accordingly towards the end of the investigation, cabinet level decision-makers will be seeking intelligence support to determine if this attack represents a major shift in terrorist's tactics away from more simpler methods such as IEDs—or whether the attack represents an increased interest or willingness to use bio-weapons and a greater capability across a particular group. At this level, presidents and prime ministers along with their senior cabinet members would be tasking higher level intelligence assessments to understand what strategic drivers have come into play that resulted in individuals or perhaps even a terrorist group being interested in procuring and using anthrax for a bio-weapon. There would be a number of strategic level questions national government decision-makers would want to know about such a scenario. Do more individuals or groups have the in-house capability to produce anthrax? Is it being stolen from BSL3 and 4 labs? How? Is it being produced in a fragile state with poor biosafety controls, where the terrorist group operates and likely has sympathizers?

Coordination

Tasking alone will not ensure that a decision-maker at whatever level they are located along the decision-making process (tactical, operational and strategic) will receive the kind of intelligence support they need at the time it is required. There can be no effective tasking without a system(s) that helps ensure that both the collection and analytical response to that tasking is well coordinated. There is no one way tasks are coordinated for all biosecurity threats and risks. Much depends on the nature of the bio-threat and risk (plant, animal, human), and whether it is unintentional or intentional. The former (unintentional) suggests less national security intelligence or law enforcement intelligence agencies would be involved with a greater responsibility for public health agencies. For example, in the case of the 2015 and 2016 outbreak of Zika virus across the US one would expect an almost exclusive response from CDC and state and local health authorities. However, a sudden, unexplained outbreak of Foot and Mouth Disease in areas where it has previously not occurred might at least initially draw in the interest of the FBI, DHS, local law enforcement along with animal health and agricultural authorities at least until more is known about the threat.

Different threat/risk profiles therefore, will bring in different health authorities, scientists and agencies with a range of intelligence capabilities to bring to the task. Does this present problems? Not necessarily. Not all biosecurity tasking needs to follow the same processes, but what is important is that coordination can occur as much as possible in an integrated manner across all three levels of decision-making: strategic, operational and tactical. Such integration is an ongoing challenge for 'Five Eyes' intelligence communities in all intelligence tasking not just in the biosecurity area. Since 9/11, there have been major improvements in the way for example tasking for terrorism has been better coordinated so that senior decision-makers have confidence that the intelligence they use has been drawn and assessed from multiple sources, and is joined together in a way where the validity of key analytical judgements have been contested and peer reviewed. The setting up

of national terrorism fusion centres such as the US National Counter Terrorism Center (NCTC) or the UK Joint Terrorism Analysis Centre (JTAC) have vastly improved the coordination of collection and analytical efforts of terrorism related intelligence.

Despite such improvements, different information communications technology platforms, legislation, organizational cultural attitudes and governance issues still conspire against a seamlessly integrated coordinated response to terrorism issues across the 'Five Eyes' (Walsh 2015). As noted earlier, the sheer size of the US intelligence community makes coordination of intelligence efforts difficult. Similarly, further away from the core national security intelligence agencies, the size and diversity of law enforcement and other agencies that might have a role in collection or analyzing relevant intelligence on terrorism is large—making coordination difficult. If such coordination issues still exist for a top priority issue such as terrorism, they also exist and arguably more so for biosecurity related issues, which are less of a priority. Again some efforts have been made both from the collection and analytical perspective, particularly in the US to provide better coordination of biosecurity tasking. These efforts have occurred at the ODNI—the details of which are discussed in Chapters 4 and 5. However, interviews of senior intelligence leaders suggest that there needs to be better coordination of intelligence efforts across intelligence agencies in 'Five Eyes' countries—as well as better coordination of non-national security sources of intelligence such as scientific research/expertise and epidemiology intelligence. Further evidence is required though on how best 'Five Eyes' intelligence communities can improve intelligence coordination of biosecurity intelligence. However, given the absence of any major attack since *Amerithrax*, political masters remain largely disinterested in bio-threats and risks including overseeing better coordination of intelligence efforts in this area. They seem content to receive periodic intelligence on potential, emerging threats that may in some cases not have been produced by the intelligence community in a coordinated manner. This can result in the delivery to the decision-maker of a less comprehensively developed picture of a particular bio-threat/risk.

It is not just the coordination processes or lack thereof that can result in poor tasking results for a decision-maker. It is also true in many cases, the complexities of bio-risks and threats are difficult for many decision-makers or even their advisors to understand. This results in either no tasking or vague requests that may not reflect actual or even potentially relevant bio-threats or risks. Intelligence agencies may find themselves unnecessarily going down rabbit holes wasting limited resources due to a decision-maker not understanding what they are tasking for. Though it might be easy to apportion blame to a decision-maker for no or inadequate tasking, the intelligence community also faces another key challenge in getting the 'tasking right' and that is the lack of knowledge about how to assess both bio-risks and threats. Better tasking and coordination of bio-threats and risks also rely on how risk and threat methodologies are being applied to the biosecurity context and whether these are sufficient in guiding tasking and coordination.

Risk and Threat Assessment

It is not possible in the space available to provide a full discussion of all risk and threat methodologies used across all the 'Five Eyes' countries. The potential threat/risks space across the one health continuum is so vast and diverse several volumes would be required to do justice to describing the various methodologies used to assess them. Additionally, I am restricted in how I can discuss specific threat and risk models used by intelligence agencies as they are generally classified. However, it is possible to discuss the broader foundational principles upon which many classified methodologies have been built. Hence, this section will discuss key factors that have been used in many risk and threat methodologies that are publicly available. The discussion will highlight how difficult applying such methodologies are, particularly because the available data for previous bio-risks and threats is generally low or non-existent, and fundamental and unresolved debates remain about the intention and capabilities of potential threat actors (threat assessment) and the consequences of bio-attacks (risks). The absence of consistently

rigorous threat and risk assessment across intelligence communities does as we shall see in Chapters 4 and 5 impact on the kind of collection and analysis intelligence is able to provide on bio-risks/threats to decision-makers.

Before summarizing some key trends in bio-risk and threat methodologies, it is important to define how the terms 'risk' and 'threat' assessment will be used in this chapter. In Chapter 1, a definition for both bio-threat and risk was included, however what follows here is a more detailed discussion of the variables that constitute bio-threat and risk in order to reduce confusion about how these terms are used in different threat and risks contexts. As Burnette suggests in his discussion of basic principles of threat assessment, confusion occurs when 'biosecurity is discussed in a bio-safety or scientific setting'. Further in his words: 'it is important to distinguish biosecurity risk from biosafety risk' (Burnette 2013: 91).

Defining Bio-risk

In broad terms, risk is 'the likelihood that an adverse event involving a specific hazard or threat will occur and the consequences of that occurrence' (Caskey and Sevilla-Reyes 2015: 45). In very simple terms, Kaplan and Garrick argue 'that assessing a risk involves answering the following questions: what can go wrong? How likely is it and how likely are we to see it coming? What are the consequences?' (Kaplan and Garrick 1981 cited in Caskey and Sevilla-Reyes 2015: 45). More narrowly, in the biosecurity and biosafety context, Burnette defines *biosecurity risks* as being 'determined by measures of vulnerability to and consequences of deliberate acts, as well as the dynamic threats that impact the system or its assets'…whereas *biosafety risks* deal with probabilities and consequences of accidents where no nefarious cause exists' (ibid.: 91). The key difference between biosecurity and biosafety risks is that while both underlie vulnerabilities and have consequences, the former is the result of deliberate acts. It is the former (biosecurity risks), which naturally full under the mandate of intelligence and law enforcement agencies and is our focus.

Assessing the risks in the biosecurity context is easier in some cases than others. For example, in a lab setting the likelihood and consequences that an employee may steal a piece of support equipment such as a lap top for their own personal use at home is maybe more 'quantifiable' than whether that same person will steal sensitive intellectual property from the lab. There is likely to be more data on the incidences of the former (i.e. common theft) and its impact—enabling the institution to improve anti-theft mitigation policies and procedures.

In contrast, the risk posed by an employee stealing sensitive intellectual property may be more difficult to calculate using conventional methods of risk assessment given there is less 'reliable knowledge about likelihood, scale, nature and vectors of harm' (Helm 2015: 103). More recently, however, Gryphon Scientific, a small consulting business made up of life scientists and health researchers, who consult on global health and homeland security issues have provided advice to the National Institute of Health on the risks posed by malicious actors and acts targeting labs in which gain of function (GOF) viruses are studies or stored, and the risks posed by the independent replication of published GOF research by malicious actors (Gryphon Scientific 2016). Their report provides a comprehensive risk assessment methodology. The methodology is a mixture of quantitative and qualitative measures based on a detailed collection of data from historical cases, hypothetical scenarios, legislation, biosafety regulations and interviewing scientists, general counsel, FBI WMD Coordinators and other law enforcement personnel. They then methodically identify potential malicious actors and the attack vectors and consequences for each. For example, in terms of the risk posed to labs undertaking GOF research by malicious actors and acts, malicious actors identified were (lone outsider, lone insider, organized criminals, domestic terrorists and extremists, transnational terrorists including state like terrorist groups and foreign intelligence entities). Attack vectors identified were multiple including for example (armed assault, bomb or arson, theft of pathogens, subversion of employee and cyber covert entry) (Gryphon Scientific 2016: 847). In-depth research and interviews of a range of experts across both the health, scientific and security sectors resulted in a threat matrix of

malicious actors, which provides a useful global way of understanding the likelihood and consequences for each act depending on the actor and vector of attack. The Gryphon study concluded that the 'most likely malicious act to be carried out in or on a containment lab include theft of virus stocks, experimental samples, equipment or research animals, deliberate contamination of personal protective equipment of lab equipment of co-workers, and mixing of infected with uninfected samples or animals outside proper containment' (ibid.: 4–5). Though they also assessed given 'the regulatory and security environment, the most *plausible* malicious acts taking place at high containment research labs would involve malicious insiders, who have authorized access to the labs and viruses contained in them' (ibid.). Gryphon Scientific concluded that 'insiders may work alone or in coordination with an outside group. Their motivations range from emotional disturbances to ideological radicalization by domestic and transnational terrorists organisations' (ibid.). The Gryphon study represents progress in developing more reliable risk methodologies that assemble empirically relevant scientific data and intelligence assessments on the intent, capability and consequences of a range of malicious attack scenarios in secure labs working on GOF influenza, MERS-Cov and SARS-Cov research.

As useful as the Gryphon study is it is limited to biosafety and biosecurity risks posed by GOF research, further up the risk scale, some of the even more complex, low probability high impact bio-risks such as a bio-terrorist attack in a major metro subway cannot necessarily be 'measured' using the same risk assessment tools we would use to assess the likelihood and consequences of someone stealing some sensitive information from a secure lab environment. Generally much more is known about the lab physical security environment, security measures and employees compared to the myriad of threat actors, vectors and consequences that could arise from such a bio-terrorism attack in an open environment such as a subway. Systems thinking from engineering could provide some assistance in understanding risk assessment in a number of complex bio-risk incidents. We will come back to the role of other disciplines, including engineering in understanding risk and improving intelligence capability in Chapter 7. Basic risk management methods are also not sufficient to assessing many complex and potential

bio-risks, particularly those posed by dual-use biotechnology as they have for the most part not occurred or are still very infrequent thereby lacking the historical data normally required to assess risk.

In brief though systems approaches from engineering may be usefully applied against emerging risks as they allow for uncertainty and complexity and accept that one cannot manage away all potential bio-risk and threats. Additionally, as Helm argues many complex risks cannot be analysed with standard data methods in part because they do not follow normal cause and effect behavior (Helm 2015: 106). For example, no one could foresee all public health, political, social and economic consequences of the 2014 Ebola epidemic in West Africa. With complex risks such as a pandemic (caused intentionally or not) there is likely to be a degree of failure in mitigating some risks. A more comprehensive systems approach that assesses: *risk, resilience* and *adaptation* in an integrated way will likely result in a holistic treatment and mitigation of many complex and potentially emerging bio-risks. Resilience or the ability to plan, absorb and recover and adapt from adverse events is important in understanding complex bio-risks as there is a need to understand the vulnerabilities to a range of sectors in a locality, region, nation or globally. The intelligence community needs to understand what are specific vulnerabilities in particular sectors such as transport, city buildings, food and water supply or airports? While managing complex risks is partly about mitigating the risks to different sectors in the economy before an event occurs, a systems approach to risk management and building effective resilience also requires an understanding of how the public and private sector can respond once an event has occurred.

Mitigating against all potential future bio-risks are impossible and policy-makers are left with tough choices about the cost-benefit analysis of mitigating against exotic high impact-low probability risks, which may not occur– or ones where attempting to mitigate against such risk in the future by for example 24 hour health screening of every passenger coming into a country would not be feasible longer term and may have an impact on the economic status of a country. Adaptation the last step in a systems approach to risk management is linked to measures to increase resilience, but seeks to extend the analysis of risk by

'incorporating various mixes of proactive and reactive measures in order to manage the uncertainty' (Helm 2015: 116).

Defining Bio-threat

In contrast to bio-risks which include vulnerabilities to both accidents and deliberate acts, bio-threats involve humans in all cases and quantifying them is arguably more difficult. As discussed in Chapter 2, policy makers, bureaucrats and the intelligence communities' perspectives of threat assessments on both offensive state bio programs and bio-terrorism have varied significantly since 9/11, which calls into question the kind of threat assessment methodologies relied upon to make such diverging statements on the nature of the threat. For example, the October 2002 US National Intelligence Estimate on Iraq's weapons of mass destruction expressed a high confidence that Iraq had an offensive bio-weapons program deemed a direct threat to the US (NIC 2002). From a non-state actor perspective, the lessons learnt from the analytical failures of Iraq's bio-weapons program, which led to a US led coalition invasion of the country seemed to have not been completely absorbed by the intelligence community if one examines subsequent public announcements on threats posed by bio-terrorists and state sponsored bio-weapons programs. For example, in an address to the Senate Select Committee on Intelligence regarding the ODNI's Annual Threat Assessment, DNI Michael McConnell said: Al Qaeda and other terrorist groups are attempting to acquire chemical, biological, radiological and nuclear weapons (CBRN) (McConnell 2008: 6).

In the same year, the WMD Commission Report established by Congress in 2008 to assess the US programs to prevent WMDs gave a time line for a biological attack stating that:

> Unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013. The Commission further believes that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon. (Graham and Talent 2008: xv)

DNI McConnell's successor, Admiral Blair while agreeing in his 2009 Annual Threat Assessment with much of the assessment made by his predecessor on the growing threat that terrorists will use bio-weapons, also suggested that such weapons may be acquired by states that do not have such programs (Blair 2009: 19).

While it is difficult to extrapolate a full understanding of threat assessment methodologies from open sources, the variations between different decision-maker statements and where the emphasis is placed on different threat scenarios (e.g. state based bio-weapons vs bio-terrorism) shows that different factors are being considered in the threat formulation process whilst others are being left out. The impact of incomplete threat and risk assessments is something we will turn to in the final section of this chapter. Suffice it to say though, improving threat assessments matter as they can as Stern (2002: 94) suggest cause decision-makers to 'choose policies whose cost exceed their benefits' as we saw in the 2002 National Intelligence Estimate provided to the Bush Administration on Iraq's WMD capabilities.

Threats can emanate from an individual or group. Threats can be: internal, external, indirect and clandestine or overt (Burnette 2013: 95). Internal threats as noted earlier are particularly worrying as they involve employees and visitors, who have authorized access to research or a secure lab environment. Dr. Bruce Ivins the number one suspect in the *Amerithrax* incident is a classic example of the 'insider threat'. While intelligence and even psychiatric analysis helped FBI investigators assess the threat posed by him, investigators are not always going to have such information particularly before a bio-incident occurs. While threat assessment methodologies try to extrapolate from previous cases to predict future threatening behaviors, in the case of biosecurity and biosafety there is still relatively few cases to extrapolate from to make current threat assessment methodologies reliable.

Burnette is correct to argue that many threat cases in the past have involved individuals with a profile of violence due to a feeling of being wronged by co-workers, an estranged spouse or some kind of animal extremism (e.g. animal rights, government policy disagreement), yet the context and scenario of each case is different (Burnette 2013: 92). In addition, then to a person's intention to commit an act of violence, how

this act evolves is also context driven. In other words, the context of each threat scenario presents different possibilities for an act of violence to evolve as does the varying capabilities of different individuals in different scenarios. It is the differences between cases as much as the similarities therefore that are crucial in refining threat assessment methodologies.

Burnette defines 'indirect threats' as being at the 'wrong place at wrong time' and could be direct threats against employees or someone the attacker has a personal connection with. He cites the 2009 case of Amy Bishop, who as an assistant professor of biology at the University of Alabama, Huntsville killed three colleagues as retribution for being denied tenure (Burnette 2013: 93). Finally Burnette describes 'external threats' as involving threats to an institution or individual from an outsider. Examples include direct threats against employees that are personally or terrorist motivated or some kind of direct attack against the lab, research institute or other related institution (ibid.: 96). We must also remember that not all external threats will involve violence against persons. They could involve stolen property (particularly intellectual property, misuse or destruction of property). Of course external attacks can also involve non research or lab institutions. The list of other potential external attacks is almost endless and could involve, amongst others: office buildings, airports, water supply, food supply and as we saw in the *Amerithrax* case the mail system.

Burnette also describes—the targeted violence process as a useful way to conceptualise how threats evolve from perhaps initially a simple grievance to the implementation of an act of violence. Understanding the targeted violence process, he argues, helps security personnel identify ways to intervene earlier before the violent attack is implemented. The key developmental phases a threat will evolve through are: *intent, ability and opportunity*. Though for each three categories there are a series of sub-categories in the targeted violence process including: *grievance, ideation, planning, preparation and implementation.* Grievance is where intent is first formed. For example, someone working in a laboratory may have a complaint about the way they have been treated or a perceived wrong. Ideation, the next phase, is where the individual identifies a course of action to remedy that wrong. This of course may not be a rational choice of action.

It is at the intent category of threat development, where hopefully pre-emptive security measures inside the lab may detect an individual's behavior or words, which suggest something is not right. For example a co-worker could observe the individual making threatening statement against their employer or another individual. Other pre-emptive measures to prevent the development of *intent* is through the appropriate security vetting and character suitability processes that employees must undergo prior to commencing and at periodic intervals in secure laboratories and other research institutions in most western countries. Such checks are not fool proof, but over time they may pick up in some cases a grievance, which can be dealt with prior to the individual further developing towards an act of violence or some other kind of threat such as theft. The next phase *ability* represents the threat actor's effort to develop a definite pathway to action. It has two sub-categories (*plan and preparation*). Planning 'involves the development of the action to be carried out and preparation is the gathering and staging of the tools and plans to carry out the action' (Burnette 2013: 98). Reflecting on our lab worker scenario, it is possible that the facilities security office may be able to pick up on some early planning and put in place mitigation measures to remove the threat or reduce the risk. Though in other situations the threat assessment process will not be able to pick up early such planning and preparation prior to the threat actor carrying out the planned action.

The final phase (opportunity), as Burnette, indicates, 'is the phase in which the actor has met all needed criteria to carry out an action' (ibid.). Opportunity consist of only one sub-category—*implementation* which is self-explanatory. Again in our lab worker scenario, opportunity represents the point where the threat actor's planned violence is carried out facilitated by vulnerabilities in the environment. It is the actor's threat process described above and the existing vulnerabilities in the environment, which provide an overall risk assessment to their actual or planned actions.

Actual acts of violence that were unable to be prevented by intelligence or law enforcement intervention underscore both the difficulty and validity of threat assessment processes in the biosecurity and bio-terrorism context. In order for threat assessments to improve their ability to assess potential bio-threats in the early phases of intent or

early planning it is clear that governments, intelligence, law enforcement agencies, universities, research institutions and bio-tech companies all need to consistently and proactively collect better information and intelligence on potential threat scenarios in order to develop counter measures or the early identification of threat actors. In the narrow context of laboratory bio-risk management, having a more strategic and proactive approach to intelligence and information collection about threats is a whole of agency response not something that can just be left to the security department. It requires that employees working in a range of both public and private agencies dealing with biological select agents and toxins (BSATs) are able identify individuals engaged in behavior that may indicate a planned act of violence or theft. Developing better threat assessments that can result in more proactive rather than reactive risk mitigation strategies also rests on the extent that the executive leadership of the relevant agency can set appropriate collection requirements in place. Good information collection that brings information sources together more quickly will improve both the validity and outcomes of threat and risk assessment methodologies.

Conclusion

It is clear from the discussion above that there remain challenges for both the 'Five Eyes' intelligence community and their decision-makers on how to more effectively task and coordinate efforts against biosecurity threat and risk issues. In some respects, such challenges are no different from other threat types and risk scenarios in cyber and the constantly evolving terrorist threat. In both areas (cyber and terrorism), technology is clearly enabling threats and risks and intelligence communities struggle to understand the nature of them given the rapidly changing trajectory of technology. As noted in Chapter 2, understanding how the rapid changes in bio-technology—much of it potentially dual-use will evolve confounds biologists/scientists involved in it let alone political decision-makers. Additionally, the current levels of uncertainty, and the relatively few cases of biosecurity

and bio-terrorism incidents compared to conventional terrorism attacks or even cyber-attacks does impact on how 'the Five Eyes' intelligence communities are tasked on biosecurity and bioterrorism issues.

Other than the biological weapons aspect of WMD and a general periodic concern that terrorist *may* make or acquire a bio-weapon, it seems that tasking against a broader potential array of bio-risks and threats is adhoc and inconsistent. This inconsistency of decision-maker's interest in biosecurity and bioterrorism issues in the policy context was discussed earlier. It can be difficult to get a decision-maker's attention on an area that produces a number of potential threat and risk scenarios, which are low probability despite them being of high impact when there are far more 'here and now' issues to occupy their minds. It remains unclear, for example how the Trump Administration 'rates' biosecurity and bioterrorism issues. Nonetheless, the 'Five Eyes' intelligence communities do have a role in making sure that biosecurity and bioterrorism issues do not fall completely off the radar.

Part of the job of any intelligence community is to manage upwards—not just accepting formal tasking from the political leadership. It is also clear from this chapter that intelligence communities (including both national security and law enforcement agencies) themselves need a better understanding of how potential bio-threats and risks may manifest themselves at the tactical, operational and strategic level. Secondary and primary sources also suggest that even formal national tasking of biosecurity threats may not be being clearly articulated and communicated to sub-national security personnel (state and local police, first responders and even the private sector), which results in further lost opportunities to create better understanding of potentially nationally significant biosecurity threats if tasking and coordination processes from the national to local levels are not working well.

Improved tasking and coordination of bio-threats and risks whether that is top down (from decision makers) or bottom up (from the intelligence community) also requires as we saw an improvement in the understanding of risk and threat, including improving risk and threat methodologies.

Conflicting and accuracy issues around multiple risk and threat methodologies applied to biosecurity threats and risks provides the political leadership with different assessments on the probabilities of

various threats and their likely impacts. The inexactitudes and sometimes lack of consistency of measuring both likelihood and consequences (e.g. do we use a mathematical approach, a quantitative, semi-quantitative or qualitative approach) to provide an overall risk assessment level of high, medium or low (Caskey and Sevilla-Reyes 2015: 51)—combined with limited resources, and workforce training issues on risk and threat means tasking and coordination of biosecurity threats is not optimal.

In other words, there would likely be more informed tasking from decision-makers if threat and risk modelling in the intelligence community was improved. There also needs to be a more common understanding between governments, labs, private sector on how acceptable vs unacceptable risks are determined and agreed upon. These decisions need to be well documented. Communicating risk decisions with all stakeholders is important and obviously important stakeholders should be informed on key risk assessment and mitigation decisions (Caskey and Sevilla-Reyes 2015: 59).

Finally the 'Five Eyes' intelligence communities as suggested need to expand their understanding of risk and threat to more comprehensive or systems approaches to avoid over-simplified, biased and linear assumptions of risk, which can result in poor decision-making by decision-makers. This is easier said than done, but many future bio-threats and risks whether enabled by bio-technology or not have unpredictable consequences and are difficult to completely mitigate against. Risk management will only by the first step and the intelligence community working with other stakeholders need to play a greater role in identifying what consequences might occur in a range of scenarios, and how they can help society also improve resilience and adaptability to actual bio-attacks as much as potential ones.

In order improve to improve risk and threat methodologies in the biosecurity and bioterrorism context an evidenced based approach to knowledge collection is critical. Arguably, most knowledge may well be outside the intelligence community and residing with the scientific community or the private sector. This is a point that will be discussed in detail in Chapter 7. As we shall see in an area such as biosecurity and bioterrorism gaining this knowledge requires also that the 'Five

Eyes' intelligence communities reflect on current collection strategies to examine whether they are fit for purpose. In Chapter 4, we will look at some of the key collection methodologies and how they are being applied to biosecurity threats and risks. The chapter will also highlight what are some of the key challenges in collecting against complex biosecurity threats and risks.

References

Blair, D. (2009). *Annual Threat Assessment of DNI for the Senate Select Committee on Intelligence*. Washington, DC: ODNI.

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

Caskey, S., & Sevilla-Reyes, E. (2015). Risk Assessment. In R. Salerno & J. Gaudioso (Eds.), *Laboratory Biorisk Management* (pp. 45–63). Boca Raton, FL: CRC Press.

Clapper, J. (2016, February 9). Statement for the Record. *Worldwide Threat Assessment of the US Intelligence Community. Armed Services Committee.* Washington, DC: ODNI.

Graham, B., & Talent, J. (2008). *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*. New York: Vintage Books.

Gryphon Scientific. (2016). *Risk and Benefit Analysis of Gain of Function Research Final Report*. Takoma Park, MD: Gryphon Scientific, LLC.

Helm, P. (2015). Risk, Resilience: Strategies for Security. *Civil Engineering and Environmental Systems, 32*(1–2), 100–117.

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

Koblentz, G. (2012). From Biodefence to Biosecurity: The Obama Administration's Strategy for Countering Biological Threats. *International Affairs, 88*(1), 131–148.

McConnell, J. (2008). *Annual Threat Assessment of DNI for the Senate Select Committee on Intelligence*. Washington, DC: ODNI.

NIC. (2002). *Iraq's Continuing Programs for Weapons of Mass Destruction: Key Judgments*. Washington, DC. From http://nsarchive.gwu.edu/NSAEBB/NSAEBB129/nie.pdf. Accessed March 15, 2017.

Obama, B. (2010). *National Security Strategy*. Washington, DC: The White House.

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.

Stern, J. (2002). Dreaded Risks and Control of Biological Weapons. *International Security, 27*(3), 89–123.

Vogel, K. (2013). *Phantom Menace or Looming Danger?* Baltimore, MD: The Johns Hopkins University Press.

Walsh, P. F. (2015). Building Better Intelligence Frameworks Through Effective Governance. *International Journal of Intelligence and Counterintelligence, 28*(1), 123–142. https://doi.org/10.1080/08850607.2014.924816.