7

Intelligence and Stakeholders

Chapter 6, explored what more the intelligence communities across 'Five Eyes' countries can do from their broader organisational levels to better identify, prevent, disrupt and treat potential and emerging bio-threats and risks. In this chapter, the aim is to survey how *external* partners and stakeholders of intelligence communities can play a greater role in helping the ICs build bio-threat and risk capability in the future. The role of stakeholders can involve building capability internally or externally to national security and law enforcement agencies.

Chapter 6 demonstrated that building stronger intelligence governance and key enabling activities is crucial to developing adaptable and responsive intelligence enterprises that are better able to interpret emerging bio-threats and risks for decision-makers. However, as discussed in the previous chapter, the 'Five Eyes' countries, cannot alone improve their understanding of complex bio-threats and risks without the input from important partners and stakeholders. As discussed in Chapters 4 and 5, intelligence stakeholders, depending on the specific bio-threat or risk can be a large and diverse number of people and institutions. Subject matter expert scientists (e.g. epidemiologists, microbiologists, forensic analysts, clinicians, public health specialists, molecular biologists,

P. F. Walsh, *Intelligence, Biosecurity and Bioterrorism*,
https://doi.org/10.1057/978-1-137-51700-5_7

agricultural scientists and veterinarians) can all be critical stakeholders for intelligence communities. Without them it would be almost impossible to see how the IC alone can fulfil its mission to identify, prevent, disrupt and treat potential and emerging bio-threats and risks.

Indeed as seen in Chapter 4 'the scientific community' brings a lot of expertise to the intelligence community about how to assess bio-threats and risks in a number of different ways and contexts. These include understanding potential risks through GOF experiments, the development of biosensors and knowledge about weaponisation, pathogenicity and transmissibility of various bio-agents. Chapter 4 also surveyed briefly the role of scientists working in epidemiology and forensics as providing central roles in the prevention, disruption and treatment of bio-threats and risks. Additionally, Chapter 5, highlighted the critical role the scientific community plays in helping the intelligence community better frame their understanding of potential threats and risks emerging from the fast paced changing biotechnology and synthetic biology sectors.

This chapter provides a thematic analysis of how important stakeholders can contribute to reducing current and emerging bio-threats and risks. In contrast to Chapter 6, which focused on what *internally* the intelligence community can do to better equip itself to manage bio-threats and risks, this chapter surveys what important *external stakeholders* can bring to the table to improve intelligence capability and to reduce bio-threats and risks themselves. Paraphrasing research impact scholar Mark Reed's definition, I define a stakeholder of the intelligence community as any person, organisation or group that is affected by or can affect a decision, action or issue relevant to preventing, disrupting or treating bio-threats and risks (Reed 2016: 41). Specifically, I am referring to stakeholders in the scientific, research, clinical, policy, first responder and private sectors that can provide capability, expertise to the intelligence community and/or contribute to biosecurity through their own actions.

In particular, the thematic analysis of the role of stakeholders in this chapter is organised around three sub-headings: *prevention*, *disruption and treatment*. Traversing the literature and interviews with a select number of stakeholders shows there that there is a large and diverse number of individuals and organisations that could potentially play a role in either preventing, disrupting or treating future bio-threats and

risks. Hence, it is not possible to explore individual stakeholders in great detail in the space available. While some stakeholders will be mentioned by name for illustrative purposes, the discussion below provides analytical generalisations of scientific innovations, techniques, research, policies and other initiatives that stakeholders can bring to improve the future capability of intelligence communities as well as contributing themselves to prevent, disrupt and treat bio-threats and risks.

Prevention

Improving Bio-Surveillance Capability

Before discussing what knowledge and capabilities various bio-surveillance stakeholders can bring to the intelligence community it is important first to define the term. Unsurprisingly, there are several definitions to choose from. In this section I have selected a comprehensive definition cited in a US GAO report.

> In the biological context, surveillance is the ongoing collection, analysis, and interpretation of data to help monitor for pathogens in plants, animals, and humans; food; and the environment. The general aim of surveillance is to help develop policy, guide mission priorities, and provide assurance of the prevention and control of disease. In recent years, as concerns about consequences of a catastrophic biological attack or emerging infectious diseases grew, the term bio surveillance became more common in relation to an array of threats to our national security. Bio surveillance is concerned with two things: (1) reducing, as much as possible, the time it takes to recognize and characterize biological events with potentially catastrophic consequences and (2) providing situational awareness—that is, information that signals an event might be occurring, information about what those signals mean, and information about how events will likely unfold in the near future (GAO 2011: 9).

This definition highlights how the functions and roles of bio-surveillance has changed from a more narrow concern of mapping disease in the public health sector to represent a diverse array of knowledge and

capabilities that are vital in understanding bio-threats in the national security context. The definition also underscores the ongoing multiple challenges in improving bio-surveillance capabilities and their utility in the national security context. Three key challenges in particular remain for improving national bio-surveillance capabilities and they are: methodological, information sharing and integration issues. The information sharing and integration issues have already been discussed in Chapter 6 so this section will focus on the bio-surveillance methodology issues. By methodological issues, I am referring to both the technical methods (biosensors) and the broader different disciplinary approaches to bio-surveillance that now inform debates amongst stakeholders on how to improve bio-surveillance capabilities.

From a technical perspective, there has been a range of bio-sensor research from inside and outside the IC to detect the release of dangerous pathogens into the environment. Perhaps the most well-known of these initiatives—Biowatch was developed by DHS in 2003 with the aim to detect aerolised bio attacks for high risk bioagents in major US cities. The program however, has had mixed success relating to the reliability of results and the delay in the publication of these once samples were collected from the field (GAO 2016, 2017). The DHS tried to speed up the detection times from the first generation manual systems to Gen 3 acquisitions, which promised speedier autonomous systems though testing difficulties remained. Further analysis, however, of alternatives by the DHS as showing any advantages of an autonomous system over the current manual system were insufficient to justify the cost of a fully technology switch (GAO 2016: 7). In the US, research continues to improve the robustness, sensitivity, specificity, timeliness and cost of biosensor equipment. While conventional PCR based methods and immunoassay are still being used other biochemical, microbiological and genetic solutions are being trialled such as the incorporation of antibodies and peptide molecules, which may greatly reduce detection times to minutes instead of several hours (Kim et al. 2015). Leaving aside efforts to improve aerolised biosensors, the expected rapid growth of synthetic biology and biotechnology and the potential (however unknown) that bioengineered material may be used maliciously in a way that threatens public safety or national security may shift the focus

into other scientific research that can detect signals of bio-engineering including types of changes, location and possibly in the future where changes were made. In July 2017, IARPA commissioned a new program—Finding Engineering Linked Indicators (FELIX) to meet such objectives. IARPA is seeking interest from a range of scientists (synthetic biologists, micro biologist, immunologist, statisticians and computer scientists) to carry out 3–5 research projects addressing the two main focus points of FELIX (Eaves 2017). If this research can produce reliable results, it will provide another useful collection and analysis point for the IC by allowing the detection of previously undetectable signatures of bio-engineered material in bio-criminal and terrorism cases.

In addition to the various technical innovations in biosensors, a range of other bio-surveillance methods have been deployed. In the late 1990s, the US CDC pioneered syndromic surveillance systems, which were initially aimed at improving the early warning of infectious diseases and bio-terrorism and have now evolved to include situational awareness (Buehler et al. 2004). Similar syndromic surveillance systems have developed in other 'Five Eyes' countries such as the UK's Real-Time Syndromic Surveillance Team (ReSST), which collects four national syndromic surveillance systems from several sources. Additionally and more recently, the Robert Koch Institute is creating an early warning system based on machine learning and natural language processing that will include 'appealing' interactive web applications and be linked to the German electronic reporting and information system DEMIS (Robert Koch Institute 2018). Syndromic surveillance systems are a critical adjunct to traditional public health lab surveillance as they strive to provide real time or near real time collection, analysis and dissemination of health data to enable early identification and management of public health threats as they are not based on lab confirmed diagnoses—and assess a wider set of health related data including: clinical signs, absenteeism, pharmacy sales or animal health production collapse (Buehler 2004). A clear benefit of syndromic surveillance is it can be cheaper, faster and potentially more transparent then a state's public health lab surveillance system. However, as with the use of big volumes of data more broadly in the IC, data quantity, quality and structural variation all impact on the utility, accuracy and timeliness of some

rapid epidemic intelligence from internet based surveillance methods (Yan et al. 2017).

Increasingly these syndromic surveillance systems rely on the use of big data, machine learning and analytics. Additionally, web based epidemic detection systems like BioCaster Portal developed by the National Institute of Informatics in Tokyo (Collier 2015) and Canada's Global Public Health Intelligence Network (GPHIN) an event based surveillance system which looks at news feeds globally have also contributed to syndromic surveillance systems (Mawudeku et al. 2015). Several event based internet surveillance systems have grown in number in the last decade. Using PubMed, Scopus and Google Scholar data bases, O'Shea's study found 50 based internet systems all using different technology and data sources to gather data, process and disseminate it to detect infectious disease outbreaks (O'Shea 2017). In line with the broader IC development of exploiting social media analytics discussed in Chapter 4, in 2013 DHS piloted another approach to bio-surveillance. The pilot involved DHS trialling various social media analytics from self-reported information on Facebook and twitter to determine pandemics and acts of terrorism given social media feeds can provide close to real time reporting of symptoms, sickness access to hospital or pharmaceuticals (Insinna 2013).

Additionally, other private companies have entered the bio-surveillance space—providing novel methods for capturing bio-surveillance data. Wilson's discussion of how a private company (Veratect Corporation) assessed signal recognition in global media reports to provide warning on the emergence of the 2009 H1N1 influenza pandemic shows how the IC warning culture methodology can be employed usefully along with what he described as the 'risk adverse forensically oriented response culture favoured by traditional public health practitioners' (Wilson 2017: 1). The Veratect case shows that the private sector has a role in developing better bio-surveillance capability as well.

As can be seen from the brief discussion above about different methodological approaches to bio-surveillance. There are also different views amongst bio-surveillance scholars and practitioners about the merits of each, particularly in their abilities to predict the 'next pandemic'. Can for example, a national bio-surveillance system informed by one or

more methods discussed above predict the emergence of the next pandemic or outbreak, particularly novel new viruses? Some scientists argue that the prediction of a micro-evolutionary process of some biological agents such as a virus (i.e. a short term emergence or cross species transition) is incredibly difficult given evolutionary and epidemiological timescales are fundamentally different. Geoghegan and Holmes argue that instead it would be better to build surveillance capability that 'assesses the fault line of disease emergence at the human-animal interface, particularly those shaped by ecological disturbances' (2017: 7).

Others have argued differently. Scientists working on the USAID funded PREDICT and the Global Virome Project examine disease hotspots globally in order to sequence (rather ambitiously) almost all the viruses in birds and mammals that could potentially spill over into humans. In particular, researchers working on the Global Virome Project believe that prediction of which viruses might spill over from animal to human health is possible. Geoghegan and Holmes in response argue focusing on disease hotspots relies on very small amounts of data that can be unreliable given they are rare events. They give the example of Saudi Arabia which has not classically been a hotspot, yet MERS recently jumped into humans from camels there. Sequencing these viruses may provide useful evolutionary information, but Geoghegan and Holmes argue it won't necessarily provide early warning of what is going to affect us (Geoghegan and Holmes 2017).

Other scientists are trying to change the ecology of disease, which presumably in some cases would make the early warning of some pandemics easier. In recent years, the scientific community has increasingly exploited CRISPR gene editing techniques to change the genetic makeup of malaria mosquitoes. Additionally, advances in gene drives have recently been shown to change the ecological parameters of disease. Gene drives are artificial 'selfish' genes that can force itself into 99% of an organism's offspring instead of the usual 50%. Currently there is a global research effort funded by the Gates Foundation to cause female mosquitoes to become sterile within 11 generations or 1 year. The objective would be to release the genetically altered mosquitoes into malarial areas by 2029 (Regalado 2016). There are concerns by the FBI however that gene drives could be misused to create a 'designer plague' (ibid.).

In addition to the 'predictability' challenges presented by various bio-surveillance methods, there are also differences in opinion amongst members of the bio-surveillance community about what an effective bio-surveillance system looks like. On what metrics can an 'effective bio-surveillance' system be evaluated given the multiple methodological approaches and systems that have developed for bio-surveillance? Clinician and public health security specialist Jim Wilson has argued that the development of an effective global surveillance and response system is probably at least a decade or more away (Wilson 2017: 222). In the interim, we are left with multiple approaches of varying validity and reliability. So based on the current fragmented bio-surveillance efforts how do we learn the lessons that need to be learnt that will enable the implementation of the long awaited national bio-surveillance capabilities? How do we know if progress is being made to that goal? Importantly, beyond national efforts, how do we assess the current capability of state, local agencies to contribute to a national bio-surveillance capabilities? Where are the gaps and vulnerabilities in the current sub-national bio-surveillance and detection systems? (GAO 2011). Compounding the current challenge of evaluating bio-surveillance capabilities in order to construct a viable national approach is that different bio-surveillance systems have been created for different end users (e.g. animal and human). The Blue Ribbon Project report into animal health detailed information sharing challenges in animal health bio-surveillance and its integration with other bio-surveillance data including in human health (Blue Ribbon Report 2017: 25). This lack of integration makes it difficult to assess how information collected for animal or agricultural bio-surveillance could improve national approaches to bio-surveillance, particularly in scenarios where the emergence of disease could be an intentional or a malevolent act.

Different approaches to bio-surveillance have been informed by multi-disciplinary perspectives, which can be both a strength and weakness to developing a national perspective. Current efforts across the 'Five Eyes' to develop fully national and integrated bio-surveillance capabilities remain works in progress and the political will to steward them into being seems insufficient. For example, in the US a program designed to provide a national bio-surveillance and integration system

was eliminated in the President's Budget Request for FY 2018 (Blue Ribbon Report 2017: 41).

Any evaluation of the effectiveness of various methods and approaches for building a national bio-surveillance capability also needs to consider how national efforts can both enhance and lever off global bio-surveillance capabilities. Gaps and impediments in global bio-surveillance have become increasingly evident to the world in the wake of the largest Ebola epidemic ever—in which these challenges impacted the ability to prevent, detect, and respond. Under the looming threat of MERS-CoV, leishmaniasis, influenza, multidrug-resistant tuberculosis, and plague, the global public health community now realizes the urgent need to address shortcomings in global bio-surveillance and the broader public health security system. Properly preparing for the next major outbreak hinges on our willingness to transform global health surveillance systems and those of countries with fragile health infrastructures (Shaikh et al. 2015: 183–186). In some respects, similar challenges in developing national bio-surveillance capabilities exist in those at the global level including: siloed systems, inadequate training and technical expertise, different information and communication technology (ICT) standards, concerns over data sharing and confidentiality, poor interoperability, and inadequate analytical approaches and tools.

There is likely not one bio-surveillance method, technique or tool that is going to detect in real time disease outbreaks, particularly unusual ones which might imply malicious intent. A fully integrated approach to bio-surveillance may rely on more than one method or capability which together can provide reliable and valid bio-surveillance data and early warning at the national and global level. It may mean investigating ways that older legacy systems can be integrated or at least made interoperable with newer more mobile platforms such as mobile or wireless health technologies particularly in the developing world (Shaikh et al. 2015). It should be clear by now that improving bio-surveillance capabilities is essential to improving the prevention of natural and suspicious outbreaks of disease. It is important for the 'Five Eyes' intelligence and law enforcement communities to understand broadly the theoretical and practical developments in bio-surveillance so that they are able to more effectively lever relevant knowledge on bio-threats and risks.

Improving National, Regional and Global Health Security Capacity

A second cluster of stakeholders that are useful in the prevention of bio-threats and risks (both natural and malicious) are those working in national, regional and global health. The Ebola epidemic (2014–2015) was a recent reminder of the consequences of weak public health capability and infrastructure in failing to prevent, identify and respond quickly to infectious disease. The Ebola epidemic also had a catalytic effect on many public health authorities, practitioners and researcher's views about the capability of the traditional UN response to global health crisis mainly coordinated through the WHO. Many public health watchers are now arguing the need for a broader more effective focus—not just on prevention and response to infectious disease, but one that also included reframing the focus as a human security issue. Adherents to this view make a compelling point when seen through the Ebola case that continues to have significant impact on the economic and social stability of countries impacted (Sparrow 2016; Marston et al. 2017; WHO 2015; MMWR 2016). Beyond West Africa, similar vulnerabilities in capabilities such as diseases surveillance, detection, contract tracing, clinical care, community engagement and communications exist globally as was also seen with the proliferation of Zika in Latin American/Caribbean and MERs in the Middle East. In 2016, the Commission on a Global Health Risk Framework for the Future that met after the Ebola crisis estimated 4.5 billion per year investment would be needed for better detection and response tools. The same Commission report also estimated that the economic cost for global pandemics per year was $60 billion (Schnirring 2016; Dzau and Sands 2016).

Effective national bio-surveillance relies on not only what 'Five Eyes' countries can do to improve the scientific and technical capability of bio-surveillance, but also how they can improve bio-surveillance globally particularly in at risk areas. Beyond effective bio-surveillance, effective prevention of pandemics whether natural, accidental or malicious relies on good global (multilateral), regional and national public health responses.

There are several multilateral instruments, institutions and initiatives that are relevant, but I will focus here on what have become the key ones rather than attempting to traverse in detail all major international health initiatives struck since 9/11. They include WHO International Health Regulations (IHR), UN Security Resolution 1540, the Global Health Security Agenda (GHSA), the Biological Weapons Convention (BWC) and the Australia Group.

WHO IHR

The WHO international health regulations (2005) entered into force in June 2007 to prevent, protect against, control and provide a public health response to the international spread of diseases (detect, assess, notify events has a biosafety and biosecurity function) and includes all 192 members of the UN. The IHR 2005 has improved accountability of countries about progress towards building national core public health capability targets in several areas including, but not limited to: surveillance systems, creating rapid response teams, border management. However, the IHR annual reporting process has been by self-assessment of core capacities to the World Health Assembly (WHA) by all state parties, which has resulted in incomplete or not credible reporting for some member states.

The Commission on Global Health Risk Framework for the Future also expressed concerns over the self-assessment monitoring tool of the IHR, because questions are binary (yes/no) answers and recommended that WHO devise a regular independent mechanism to evaluate country performance against benchmarks (GHRF Commission 2015: 33). For example, a country can 'tick yes' for having a national public health legislation, but other dependent legislation (biosecurity, food safety, environmental health) may not be in place—thereby reducing overall the country's ability to manage health crisis or for the global community to understand and respond to capability and information gaps in that country (ibid.). Some countries continue to be slow or uneven in their reporting of IHR (2005) attributes. In 2013, one study showed that the African region was well below global averages across all attributes measures with no African state reporting full implementation (Kasolo et al. 2013: 11–13).

Biological Weapons Convention (BWC)

The second multilateral instrument relevant to our discussion here is the UN Security Council Resolution 1540 (2004), which calls on all 192 states to prohibit non-state actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their delivery systems.

More importantly and specific to bio-threats only, the BWC has historically played the most significant role in preventing the weaponisation of biology. The BWC was established in 1972 and seeks to prohibit the development, production, acquisition, transfer, stockpiling and use of biological and toxin weapons (Gerstein 2013; Chevrier and Spelling 2016: 331–356). In 2001, there was an attempt by some member states to introduce a verification process, but this was vetoed by the US following inspection of Soviet sites under the Tripartite agreement between the Soviet Union, USA and the UK. The US arguing it could be difficult to certify that a state's biological program was merely defensive rather than offensive. The US also had concerns that inspection to labs could be disruptive or provide opportunity for industrial espionage against legitimately operating biotechnology companies (Gerstein 2013: 137). Historically there has been a mixed record by some 'Five Eyes' intelligence countries in assessing verification and therefore non-compliance of the BWC. Koblentz surveyed the role of intelligence (particularly HUMINT) in assessing the former Soviet Union's offensive bio-weapons program between 1971 and 1990 which resulted in an incomplete picture of Moscow's program (Koblentz 2009: 157). Additionally, as discussed in Chapter 2, in 2002 several 'Five Eyes' intelligence communities (US, UK and Australia) incorrectly assessed that Iraq had a mobile offensive bio-weapon capability. Intelligence collection on its own can either over or under-estimate such capabilities.

Between 5 yearly review conferences, several initiatives and activities have been introduced (confidence building measure, meetings of experts, information exchanges) to improve the effectiveness and the implementation of the Convention. However, state parties are only encouraged to implement relevant national legislation and other measures to prohibit prevent the development, production, stockpiling or transfer or use of bio weapons. How they precisely undertake measures

is at the discretion of individual state parties. The BWC has been criticised for several reasons over the years. Some of this is warranted, while other criticisms seem to not take into account that the BWC is different from its chemical and nuclear counter proliferation counterparts. As Gerstein argues, 'material is the centre of gravity for nuclear discussions and intent being the center of gravity for biological issues' (Gerstein 2013: 176). Developing nuclear weapons leaves a large recognizable footprint, whereas the development of an offensive biological weapon requires virtually no specialised equipment (ibid.).

The first major criticism of the BWC is that it has no verification mechanism or any other mandatory provisions for monitoring compliance. A second complaint is that for many years (until 2006), it lacked an implementation capability to help states fulfil their obligations. Since 2006, the Convention has had a small three team Implementation Support Unit (ISU) based in the United Nations Office for Disarmament Affairs in Geneva which aims to 'assist, coordinate, and magnify the implementation efforts of the States Parties to help States Parties help themselves' (Lennane 2011: 85). In reality though, the ISU does not have 'capacity for analysis and coordination other than for the collection of the annually submitted confidence building measures, posting them to the website and organising and attending conferences' (Gerstein 2013: 173). Historically there has also been a low number of party states submitting their annual confidence building measures. Although the BWC ISU was able to report that a record number (81) annual confidence building measures were submitted in 2016, this only represented 45.5% of all 179 state parties submitting that year. Though the trend line seems to be going up from a low in 2014 of 19 (*BWC Newsletter* 2017: 3).

A third criticism of the BWC is that it has moved slowly since inception and further questions remain about its relevance strategically and operationally in preventing bio-threats and risks into the future. Such questions are likely fundamental to its long term viability. However despite shortcomings, the BWC has nonetheless created a normative institution for reducing the risk of biological or toxin weapons being used or developed by state and non-state actors (Lennane 2011: 85). More importantly, as developments in biotechnology continue at a pace, the BWC does provide a venue, where the security implications of

dual-use technology can be assessed which will be critical in 'mitigating these emerging threats' (Gerstein 2013: 175). The BWC still does have an important role in reducing weaponisation of biology in the future, though its poor funding particularly of the ISU means that other multi-lateral measures are needed to amplify the work of the Convention.

The Proliferation Security Initiative and the Australia Group

In addition to the above historic/traditional proliferation arrangements of the BWC, other international regimes have been implemented such as the Australia Group (established in 1985) and the Proliferation Security Initiative (established in 2003). Both have a broader counter proliferation objectives beyond biological weapons to chemical and nuclear. The Australia Group 41 member countries have collaborated on the development of lists of technologies and materials that could be used in the development of chemical and biological weapons. Member countries then commit to monitor the export or transfer of these materials. The Australia Group maintains common control lists for dual use bio-equipment, technology, software, bio agents and plant and animal pathogens as the basis for promoting common standards and regulations (Australia Group Common Control List Handbook 2015). The Australia Group works in concert with the BWC. The PSI was a Bush Administration initiative that sought to supplement existing non-proliferation regimes, but seeks to enforce these by interdicting and seizing illegal weapons or missile technology in planes or ships carrying cargo. The PSI also includes intelligence sharing and joint operational activity (National Institute for Public Policy 2009).

Global Health Security Agenda (GHSA)

Turning the focus slightly away from multi-lateral counter proliferation measures, other multilateral initiatives have focused on improving global health security. In some respects the GHSA provides a bridge between traditional, narrow security approaches to biological weapons

and a wider securitisation of global health. The GHSA was established in 2014 by the Obama Administration and is a multi-sectoral approach to global health security seeking to include governments, international organisations and non-government organisations. GHSA was set up in part to 'advance further the IHR implementation through focused activities to strengthen core capacities and to ensure a world safe and secure from global health threats posed by infectious disease; where we can prevent or mitigate the impact of naturally occurring outbreak and intentional or accidental releases of dangerous pathogens' (Heymann et al. 2015: 1889). GHSA is a refreshing approach not only because it seeks to establish a global framework and capacity to assess, measure and sustain advances in global preparedness for epidemic threats, but it also addresses biosecurity as a public health priority—thereby linking public health and health security, development, defense and agricultural sector (Cameron 2017). The underlining logic of GHSA suggests that the same attributes needed to prevent, detect and respond to deliberate use of a bio agent are those required to manage a natural or accidental outbreak of a biological agent. GHSA also includes 12 technical targets aligned to three areas: prevention, detection and response (Heymann et al. 2015: 1889). Like earlier initiatives, such as the US sponsored Global Health Initiative (GHI), which was discontinued by the Obama Administration in 2012 due a lack of financial and technical authority to leverage and coordinate multiple US agencies—the GHSA will need to secure ongoing funding beyond 2019 from major donors including the US. At a November 2017 GHSA ministerial meeting in Uganda, assembled governments signed onto an extension of the GHSA for another five years. US Secretary Tillerson had issued public support for continuing it, but at the time of writing no commitment by the US for future financial support (beyond FY 2019) has been made. GHSA holds promise, but in addition to ongoing funding challenges, those member states signed up to it will need to ensure effective governance is in place to align funding to global health priorities articulated by the WHO, World Bank, IMF and other donors in order to avoid duplication and promote an effective approach to international health security capabilities (Paranjape and Franz 2015; Schnirring 2017).

In summary, this discussion of multilateral security and global health initiatives demonstrates that there is a diverse number of stakeholders working in these sectors, which can play a role in preventing bio-threats and risks—whether they are natural pandemics or a malicious attack from a biological weapon. It's clear that the 'Five Eyes' intelligence communities have worked extensively with other member states in counter-proliferation institutions such as the BWC and the Australia Group for several decades, but what remains still under developed is how global health security stakeholders and intelligence communities can work more collaboratively for the mutual goal of global health security regardless of whether the risks are natural pandemics or result from a bio-terror attack or theft of a dangerous select agent from a lab. More trusting and formalised contact between both global health security stakeholders and those working in the security and intelligence communities can only be mutually beneficial to preventing major bio-threats and risks.

Stakeholders and Their Own Biosafety Procedures

The final cluster of stakeholders that can help prevent bio-threats and risks are of course those that specialise in biosafety and its promotion in their research institutes, biotechnology companies, universities and medical facilities. Promoting biosafety in environments that work with select agents and other facilities that work with less dangerous material which can still cause harm relies on consistently high risk management practices. In all 'Five Eyes' countries there has historically been in place biosafety risk management procedures and practices to prevent accidental infection, accidental release, or intentional misuse of biological substances. However, as noted in Chapter 2 in the last two decades the expansion in synthetic biology, biotechnology and biological science research has meant there are now more people working in more locations on dangerous pathogens—not just in well-regulated liberal democracies such as those in the 'Five Eyes' countries, but also in developing countries; where biosafety and biosecurity capabilities and practice may be less established such as parts of Africa, the Middle East,

Pakistan and former Soviet states (Gronvall et al. 2016; Shinwari et al. 2014). Just in terms of the scale of this expansion of facilities working with dangerous pathogens—in the US alone, there is thought to be thousands of BSL 3 labs and in China the number of such labs is increasing too (Nature Editorial 2014: 443).

The US and other 'Five Eyes' countries such as Canada have invested in cooperative engagement programs since 9/11 in several former Soviet Union states. The US Defense Threat Reduction Agency (DTRA) has lead efforts in Georgia to reduce bio-risk by securing/consolidating pathogens, training scientists in biosafety and biosecurity technology, regulation and detection. Likewise, the CDC has been involved in building public health capacity there as well as in Armenia and Azerbaijan (Bakanidze et al. 2010: 7). As important as building biosafety capacity is in developing countries, it is clear that much more still needs to be done to build biosafety capacity in 'Five Eyes' countries—including finding better ways to understand and manage comprehensively threats and risks in the biosciences environment.

Biosafety experts such as Salerno and Gaudioso argue for more comprehensive risk management systems across the global bioscience community 'to avoid an accident that jeopardizes the entire bioscience enterprise' (Salerno and Gaudioso 2015: xv). Their argument is that such a system would supplement existing national and international biosafety regulations by risk managing fully at an organisational and unit level every single potential incident rather than by generic risk hazard assessments that are currently done by most facilities today (ibid.: 201). Others have also called for more systematic tools and approaches for managing biosafety incidents in labs dealing with particular dangerous pathogens such as Marburg Virus (Dickmann et al. 2015). Still others have argued that while 'security awareness is high among employees who work with biological select agents and toxins, it is not pervasive across the entire life research community' (Grphyon Scientific 2016: 1014).

Such a statement does not seem to be hyperbole if one looks at some of the cases of biosafety and security lapses since 9/11 (GAO 2009, 2013). There have been several lapses at CDC between 2014

and 2016. In June 2014, dozens of workers in CDC could have been potentially exposed to live anthrax that hadn't been killed before being shipped from CDC's Bioterrorism Rapid Response and Advanced Technology (BRRAT) BSL 3 to a BSL 2 lab in its Bacterial Special Pathogens Branch. CDC investigations determined that at least 67 CDC staff members may have been exposed to viable anthrax cells or spores though no illness or deaths occurred (CDC 2014). The same report found several breaches of biosafety process and procedure including failures of policy, training, supervision, judgement and even scientific knowledge (ibid.). Similarly, biosafety lapses cases involving CDC labs occurred in January 2014 when an unintentional cross contamination strain of low pathogenic avian influenza A (H9N2) with a strain of highly pathogenic avian influenza A (H5N1) was shipped from CDC to the USDA (Schnirring 2014). Further biosafety breaches were detected in July 2014—this time at the National Institute of Health campus in Bethesda Maryland; where 6 viable smallpox vials were discovered improperly stored (Dennis and Sun 2014a). An additional five improperly stored vials were also found at the NIH—three were select agents (*Burkholderia pseudmomallei, Francisella tularensis and Yersinia pestis*) (Dennis and Sun 2014b). In the NIH cases despite their age, they were still viable organisms which could have caused illness. Their theft could have also posed a bio-threat and risk to the community.

Then after a hiatus where biological material was suspended being sent between BSL 3 and BSL 2 labs live transfers commenced again. After a further internal CDC review (CDC 2015a, b) some additional safety measures were put into place, however there was a subsequent lapse when a specimen of Chikungunya virus was shipped from a high secure lab in Fort Collins to a lower level one which had not been killed (Young 2015). Similarly, in 2015 the Pentagon shipped live anthrax spores from the Dugway Proving Ground in Utah to 9 states and one international location that were also meant to have been killed (Burns 2015). It was later found that Dugway and the US DOD had been shipping nationally and internationally live anthrax for more than 10 years—often without adequate safeguards. Other reports suggested that some samples were sent by Federal Express (Sisk 2016). Similarly in November 2016, the US HHS discovered that a private lab had

'inadvertently sent a toxic form of ricin to one of its training centres multiple times since 2011 putting training staff at risk' (GAO 2017: 1). Similar biosafety lapses have occurred in the UK resulting in 75 investigations since 2010 of government, university and hospital labs (Sample 2014).

As noted in Chapter 2, one possible bio-threat and risk pathway could be the theft of biological substances or information from a biosciences institution. Lapses in biosafety arrangements demonstrate, at least in some cases, biosecurity vulnerabilities that could make the theft or even infiltration of a threat actor into high containment lab easier. Thefts from labs have occurred in the past by an insider, and a motivated insider can compromise biosafety for a range of reasons. Bunn and Sagan's edited book *Insider Threats* provides a useful taxonomy for thinking about 'insider threats' (Bunn and Sagan 2016). They can be: self-motivated insiders, who at some point decide to become a spy or thief. Insiders can also be recruited insiders, who are already inside an organisation, but become convinced to become part of a plot. Finally, an infiltrated insider might be associated with some adversary of the organisation and join it with the purpose of carrying out a malicious act against it. Bunn and Sagan also refer to inadvertent or non-malicious actors, who pose a threat by making mistakes without really intending to do so—such as leaving a password lying around. Finally, the authors refer to a 'coerced insider', who remains loyal in intent, but knowingly assists in theft or sabotage to prevent hostile acts against themselves or their loved ones (ibid.: 4).

The insider threat that was posed by Bruce Ivins' activities in a high containment lab (that resulted in *Amerithrax* in 2001) demonstrates the potentially high threat and risks associated with an insider. The Ivins case provides a useful case study in how an organisation's security procedures and other organisational and cognitive biases can miss for several years risks posed by an insider threat actor (Stern and Schouten 2016: 74–102). Since the *Amerithrax* incident, significant investment has been made to close the biosafety vulnerabilities revealed by it.

Increasingly since 9/11 and *Amerithrax*, a number of policies, procedures and normative behaviour have developed in the scientific community to promote biosafety and biosecurity. These have ranged from

safety regulation codes such as the US *Biosafety in Microbiological and Biomedical Laboratories* (*BMBL*) to more formal legislative and oversight regulations. The latter will be addressed in Chapter 8. There are also technical and policy improvements that can be made in securing both physical and remote access to labs including computer systems that house data, which are at risk of theft or being hacked (Gryphon Scientific 2016: 1014; Berger 2013: 113–127; Slayton et al. 2013: 51–70).

Leaving aside discussion of some of the formal legislative and regulatory instruments for promoting biosafety, the development and maintenance of effective risk management across the biosciences also relies on an organisational culture that treats biosafety and biosafety as an equal priority to other deliverables. A culture of accountability at all levels must also exist if effective risk management can prevent, identify and treat bio-threats and risks promptly. A rogue insider threat, who may have been assessed as appropriate to work with select agents and seems initially to follow all the relevant biosafety regulations and procedures could still pose a risk if they have not embraced the organisation's normative cultural biosafety values. It is critical then in order to stop opportunities for insider threats, that the organisation promote relevant biosafety cultural values as much as and perhaps more than adherence to formal biosafety regulations.

Risk management measures must of course be measured against the ability of scientists to carry out its functions. Effective engagement with local law enforcement and relevant domestic security intelligence organisations in each 'Five Eyes' country to help scientists build viable biosafety cultures will likely remain important in addition to internal organisation biosafety initiatives. Stern and Schouten provide a number of useful suggestions for improving policies and procedures that may help improve biosafety cultures across the biosciences enterprise (2016: 101–102). Two that I think would be helpful are, one: developing standard operating procedures for proactively identifying vulnerabilities including using 'red team' exercises to explore how systems could become exploited. In other words, what motivators (financial, psychological, religious, and political) might drive an insider threat and are there ways to assess the signs of such an evolving threat? The other

is to 'ensure personnel reliability programs incorporate ongoing assessments of counterintelligence vulnerabilities, including vulnerabilities to self-ascribed whistle-blowers or attention seekers' (ibid.: 101).

Effective biosafety and biosecurity training is also crucial as the number of labs working with select agents or other dual use bio-agents proliferate globally, particularly in locations with fragile states. More consistent approaches to training will also be important so nations can be confident that as many scientists as possible regardless of the country or the context in which they work understand what bio-risks and threats may emerge and how to prevent or mitigate against them (Sture et al. 2012).

Disruption

As discussed above there are multiple stakeholders in the scientific community, global health security and biosafety fields that can play a critical role themselves in preventing bio-threats and risks as well as supporting the operational efforts of the intelligence community to prevent these. While prevention of bio-threats and risks is one critical dimension that stakeholders can play central roles another is disruption. Although the intelligence community can use a range of knowledge, technologies and methodologies from stakeholders in the scientific community, to prevent bio-threats and risks, we have to accept that it will not be possible to detect every criminal or terrorist act.

Nonetheless, some of the techniques, practices, technologies and knowledge available from stakeholders in the scientific community will still be useful to disrupting bio-threats and risks. In other words prevention may not always be possible yet measures can be put into place—which can detect threats early enough to reduce their impact. Similar to preventing bio-threats and risks, disrupting them will also rely on seeking advice from stakeholders involved in bio-surveillance, public health and biosafety research, amongst others on disrupting them as well. For example, as discussed earlier IARPA's commissioning of research into detecting signals of bioengineering changes (FELIX) may result in better capability for the intelligence community in not only

preventing bioengineering changes that make it easier for terrorists to carry out attacks on populations, critical infrastructure or biotechnology companies, it could also help detect and disrupt the planning stages for such attacks. Additionally as noted earlier, if a high containment lab has a strong biosafety culture it is more likely that disruption of a bio-threat may be possible just by colleagues speaking up about suspicious activities in their working environment rather than any elaborate disruption knowledge and techniques, procedures the intelligence community might have in place to disrupt such threats. But knowledge, technologies, techniques and practice for disruption of bio-threats and risks cannot just come from scientific stakeholders in the biosciences, it should also come from other fields and practitioners working in other areas where successful disruption operations has taken place. These areas include criminology, policing, engineering, legislation, cyber, counter-intelligence amongst others.

In this section, we examine briefly what other stakeholders and discipline perspectives might the intelligence community learn from that can provide better capabilities for the disruption of bio-threats and risks. Are there lessons to be learnt from other stakeholders, disciplines or even other threat contexts that might be relevant to disrupting bio-threats that might not have been initially detected? Since 9/11, there are three stakeholder and discipline groups, which are investigating and applying disruption strategies to threats and risks and their knowledge might be relevant in disrupting threats and risks in the bio context. These are criminology, counter-terrorism and cyber. We will explore each briefly to see how stakeholders (researchers and practitioners) have developed disruption strategies in each and how they might be employed against bio-threats and risks.

Criminology

Insights from criminology and the practical application of disruption for crime prevention has provided a supplementary approach to traditional law enforcement approaches of prosecution against certain crimes through the courts. Disruption is not a new concept in criminology and law enforcement practice, though it can be difficult to define in all law

enforcement contexts (Ratcliffe 2008: 204). Its meaning at least in the criminology/policing/law enforcement contexts can partly be traced back to broader desires—initially by UK law enforcement followed later by other 'Five Eyes' countries in the late 1990s and early 2000s to move law enforcement away from its traditional reactive mode to offending to one driven by intelligence. This concept of law enforcement or policing being intelligence driven or led gained significant traction in the criminology and policing literature (Walsh 2011; Ratcliffe 2016; Innes and Sheptycki 2004). It was driven initially in the UK by the desire for governments to maximise efficiencies and reducing costs by increasing the use of intelligence to drive strategic and operational decision-making. The implementation of intelligence led policing models into operational policing across 'Five Eyes' countries has had mixed results partly due to cultural, financial and leadership issues in agencies that have attempted to put intelligence at the centre of strategic and operational decision making in policing (Walsh 2011; Ratcliffe 2016). Nonetheless, despite historical challenges in adopting intelligence led approaches, increasing fiscal constraints and the ever increasing demands on law enforcement in managing both high volume crimes and complex operating environments in counter-terrorism, cyber and organised crime meant, at least in many national law enforcement agencies; a greater demand for an intelligence driven approach (Walsh 2011). This intelligence driven approach, which promulgated proactive disruption of crime strategies was in part an admission that not all crime could be prevented or the offenders prosecuted.

Additionally, in many law enforcement agencies such as the Australian Federal Police (AFP), the growing volumes of information collected have given intelligence a more central role in triaging the significance of information, value adding to it and guiding investigators to targets and operations that are high priority; or have the greater likelihood of successful prosecution outcomes. In complex organised crime cases such as transnational drug trafficking, people smuggling and even terrorism and cyber threats, which we discuss shortly—intelligence driven disruption strategies have become increasingly popular for many 'Five Eyes' law enforcement agencies. This has particularly been the case where it can be difficult to dismantle completely the organised

crime group—or to even know the full extent of the group's network. Disruption operations that attempt to take down threat actors with key roles (e.g. facilitator, financier, and logistics) may nonetheless reduce the threat posed by the organised crime network even if the network continues to exist. Additionally, with some organised crime networks, it may be difficult to secure sufficient evidence for prosecution against a more serious offence such as drug importation, but there may be sufficient intelligence that can be used to make the criminal environment more hostile for the group's illicit enterprise by arresting key group members for lesser offenses such as unexplained wealth or migration irregularities. While disruption of crime does seem like a useful tool in preventing or reducing the impact of offenders, the criminology literature demonstrates it has been difficult to evaluate the effectiveness of intelligence driven disruption strategies. Ratcliffe cited an RCMP disruption attributes tool, which attempts to examine where the disruption activity is aimed at (core business, financial, personnel) and whether the kind of disruption for one or more of these attributes is high, medium or low in impact (Ratcliffe 2008: 207). However, such tools are largely subjective and qualitative—making it difficult to accurately measure the impact of intelligence driven disruption measures. The other concern about disruption strategies is that they may just cause displacement, where other criminal enterprises take the place of those removed by law enforcement or as Innes suggest, 'disrupting a network may just provide a vacuum for more dangerous offenders to step in' (Innes and Sheptycki 2004: 14). Finally, the literature suggest that employing effective disruption strategies rely on proactive collection and valid analysis that can led to both timely strategic and operational outcomes that in turn result in threat mitigation and harm minimisation.

So are there benefits for the intelligence community working on bio-threats and risks to investigating research and practice for disrupting threats in the organised crime context? The answer is a qualified 'yes'. Much of course depends on the nature of the threat and risk posed. Clearly as with any crime, it is hard to disrupt a bio-threat, when it's still in the head of the offender. However, we do know that criminal and terrorist acts don't just happen spontaneously. There usually involve predicate steps taken by the offender. Some of these

might happen in very compressed periods while in other offences planning may take years. Either way, and regardless of whether these can be detected by the intelligence community, there is likely to be some signs in the predicate planning stages of an impending threat/risk that can provide the intelligence community opportunities for disruption. It is difficult to say in which bio-threat cases disruption strategies will be most successful. Much will depend on how quickly the intelligence community can collect and analyse information that may be indicative of an evolving bio-threat and risk. As discussed previously, good collection and analysis is contingent on having robust core intelligence processes in place and more importantly effective intelligence governance. Both are needed to ensure intelligence efforts are coordinated across multiple internal intelligence community stakeholders, with relevant knowledge—as well as ensuring information and expertise from external stakeholders (the scientific community) is available to provide earlier warning signs of an emerging bio-threat.

While it is important not to over-play the potential for success of the kind of disruption strategies used against traditional organised crime groups, there are likely bio-threat scenarios where disruption strategies may make a difference. Arguably, disruption of bio-threats could be on a continuum with the individual threat actor on one end and a sophisticated organised group on the other. At the individual level one could have the scenario of a lone terrorist actor or a mad/bad scientist. While it may seem difficult to get early warning of the malicious act of mad/bad scientist, we saw in the earlier discussion on 'insider threats' that it may be possible to disrupt their activity before you reach an *Amerithrax* style attack. Twenty/twenty is hindsight with the Bruce Ivins Amerithrax case, but the lessons learnt from this incident do provide guidance on the sources of collection and analysis required from within the intelligence and scientific communities to aid the disruption of this kind of bio-threat. It does not mean that all similar cases of 'insider threats' will be detected, prevented or disrupted, but a more careful collection and analysis of 'odd' behaviour or unusual security lapses by a scientist working in a high containment lab could reveal areas of vulnerabilities. Detection both of abnormal changes to an individual's psychological profile and/or in their working environment can provide

opportunities for those vulnerabilities to be disrupted. At the other end of the bio-threat scale, a more organised bio-criminal or terrorist planned event may resemble in some respects other illicit criminal markets and networks (drugs, identity fraud, money laundering) and thereby present opportunities for disruption. Again this is not to suggest that disruption of organised bio-threat scenarios will be always be possible. As discussed in earlier chapters, since 9/11, even with state based WMD programs the intelligence community has had a mixed record in detecting them and uncovering the intention and capability of non-state actors to exploit dual use technology for malicious end remains difficult.

However, disruption could be useful in some bio-crimes where there is a bigger network of actors involved in the illicit business. For example, in crime scenarios where food suppliers are not registered legally to import food into a 'Five Eyes' country because it poses a biosecurity risk, there may be opportunities for parts of the intelligence community (particularly national law enforcement agencies) to work with agriculture, animal health, food regulatory agencies and relevant scientific stakeholders to disrupt illicit food suppliers from a country of concern. Equally there may be opportunities for disruption of activity from non-compliant biotechnology providers in a 'Five Eyes' country, who provide dual use equipment to a company overseas with a questionable profile that resides in a country vulnerable for terrorist infiltration.

Counter Terrorism

In addition to useful knowledge that can be gained from criminology and law enforcement practice there are also perspectives on disruption from contemporary counter terrorism studies that may have utility in the bio-threat and risk context. As noted above, since 9/11 law enforcement agencies across the 'Five Eyes' countries have been increasingly deploying disruption strategies in countering terrorism given the preservation of life demands an earlier interception of attacks preferably at the planning stage. As Innes suggest in the case of counter terrorism operations, one aim is to overtly disrupt planned attacks, which has many effects including sending a message to other terrorist groups that they

may be next, reassuring the community and if possible deploying countering violent extremism (CVE) strategies in communities where future attacks may arise (Innes et al. 2017: 253). In the UK in particular, a key plank in its counter terrorism strategy has been disruption both at the strategic and tactical level. At the strategic level, disruption has involved a number of initiatives from arresting persons of interest, legislative action and enhanced surveillance (Innes et al. 2017: 265).

In addition to global influence of groups such as Al Qaeda and Islamic State, the growth in lone actor attacks—some 198 across the US and European countries from 1970s to late 2000s (Danzell and Montanez 2016: 136) has also been a significant catalyst for enacting further stringent legislative measures such as detention without trial and control orders (Walsh 2016). All 'Five Eyes' countries have also adopted further legislative changes that allow disruption of terrorist attacks by reducing thresholds law enforcement and intelligence agencies need for reasonable suspicion in order to access both electronic and human intelligence (HUMINT). Governments desire to do something to reduce the threat and risks posed by terrorists by creating increasingly proactive, flexible and permissive legislative environments has also raised concerns about the role of intelligence, secrecy and privacy. These issues will be discussed as they relate to the bio-threat and risk context in Chapter 8.

But legislation is only one plank in effective counter terrorism and the scale and pace of actual and potential terrorist attacks suggest other disruption strategies are required at the tactical level. Innes et al. suggest such strategies might include: 'prosecution against an individual or a network for offences other than those they were principally being investigated for and/or interfering with the operations of the criminal enterprise in cases where there is insufficient evidence to secure prosecution' (2017: 265). They add that, at the tactical level, disruption strategies can 'interfere with the ability of suspected adversaries to operate effectively and efficiently' (ibid.). Innes et al. suggests that tactical disruption functions at 'near event interdiction', which can mitigate or minimise harms associated with the actual or planned terrorism attack (ibid.). Other counter-terrorism disruption strategies in 'Five Eyes' countries

have included the creation of CVE policies and interventions as well as the disruption or take down of social media venues advocating politically motivated violence or recruitment to jihadist groups.

Regardless of the complexity of post 9/11 terrorist attacks—such as the multi-site attacks in Paris 2015 orchestrated by a group; or the knife attack against two police officers in Australia in 2014 by one individual—disruption strategies employed by law enforcement and national security intelligence agencies are also likely to be usefully employed in the bio-threat and risk context. Just how useful strategic and tactical disruption strategies used in conventional counter-terrorism will be in the bio-threat context depends on the nature of the intent and capability of individual threat actor(s) and the risks posed by their actions. The effectiveness of disruption strategies in the bio-threat context like conventional terrorist attacks are contingent on a range of variables that are unique to that event. In the bio-threat context, leaving aside large levels of uncertainty about the future threat trajectory for bio-terrorism, effective disruption will rely on law enforcement and intelligence agencies understanding how the intention, capability and opportunities of threat actors operating in a particular environment—make an attack possible. Intention, capability and opportunities will differ along the threat continuum from individual to group and from state to non-state actor. For example, in the research facility, hospital or high containment laboratory environment, intention, capabilities and opportunities may be shaped by actors that are internal, external or an indirectly involved in the facility (Perman et al. 2013: 95). Threats can also be as Perman suggest overt or clandestine (ibid.). In some cases, if a scientist is motivated politically (for religious, environmental or political reasons) to commit an act of violence by using a biological agent it may be easier to disrupt their activities if they are public about their agenda. However, in the case of a clandestine plan it could be very difficult to disrupt an attack launched externally or internally in a contained lab.

Nonetheless, as we saw with historical cases of lone actor threats such as the Bruce Ivins *Amerithrax* incident there are likely predicate steps in the process to carrying out an attack which are revealable. Similarly, in the lesser known case of Dr. Larry Ford, who was suspected of murdering his business partner in a biotech company—the police subsequently

found a cache of weapons, white supremacist writings and allegations that he attempted to infect six mistresses with biological agents (Perman et al. 2013: 94). Again even in cases of lone actors such as this whose attack planning is more clandestine; there may well be an abundance of 'warning intelligence' that if collected and assessed in time might be useful in disrupting a lone actor planned attack. While it can be difficult to disrupt a lone actor plot, more elaborate ones by a group of conspirators could in some circumstances provide greater opportunities for interception and disruption by law enforcement and intelligence agencies. This is because in plots involving multiple actors there are more stages before the attack can be carried out. Some stages such as communications, procuring supplies and transport also provide points of vulnerability, where threat actors can be exposed to authorities and disrupted. So an external threat such as a terrorist attack against a high containment laboratory might involve communications amongst group members, financing of the plan, purchasing of explosives and surveillance of the facility's perimeters. Each stage presents opportunities for disruption providing intelligence and information is available to law enforcement and intelligence agencies. Similarly a theft of intellectual property or biological material from a private sector biotechnology company might result from either an external criminal group; or state actor pressuring or paying an employee to steal information on their behalf. Again, intelligence may exist already about the criminal group or the compromised employee that provides opportunities for disruption.

In an ideal world of course, it would be desirable if all potential biothreat and risk scenarios could be prevented early in the intent stage, where they are mainly an idea in a perpetrator's head. Pre-employment screening, including criminal checks and select agent risk assessments will show up some individuals, who are not suitable to access and work with dangerous biological agents. This will have an early disruptive effect but it is not fool proof. People can lie about their circumstances in security suitability checks allowing them the ability to access and plan malevolent acts in a secure biological facility rather than just thinking about them. Once operating inside a facility—depending on the nature of the planned attack it can be very difficult for law enforcement and the intelligence community to respond quickly enough to disrupt the

attack before its fully implemented. In all threat scenarios (simple to complex) in addition to the mandatory background checks for workers, each scientific institution needs to develop a full suite of threat assessments that can be updated regularly on different threat actors, including but not limited to: visitors, criminals, lone actor attacks (internal and external), terrorist and issued motived groups, international terrorists groups and foreign powers (Perman et al. 2013: 94). These threat assessments should be developed by an institution's internal security department in collaboration with local law enforcement. The relatively low number of threat scenarios that have taken place involving bio-agents since 9/11 will likely mean that there will be many intelligence gaps in assessing the intent, ability and opportunity of different threat types. However, providing baseline threat assessments will begin to build pictures of threats scenarios that should help promote better biosafety measures as well as opportunities to disrupt threats earlier should they begin to emerge.

In summary, law enforcement and intelligence agencies working on bio-threats and risks of the future can learn a lot from their counter terrorism colleagues. Since 9/11, countering terrorism continues to produce lessons for the law enforcement and intelligence communities on how more effectively to disrupt emerging terror plots before they are implemented. The knowledge gained from investigating conventional terrorism attacks that don't involve biology can help those working on future bio-threats and risks by seeing how to optimise the legislative, intelligence, investigative and community response to terrorism while also learning lessons from contemporary counter terrorism efforts. In particular, the increase in lone actor terrorist attacks in the west—often with short notice underscores that either an insufficient amount of intelligence or types of intelligence that cannot be revealed in court often exists. In these cases, other tactical disruption strategies are gaining traction amongst 'Five Eyes' countries to mitigate the threat and harm posed by terrorists. Similarly, given the complexity of threat scenarios that could arise from the exploitation of dual use biotechnology, it may be difficult in some cases to collect sufficient solid 'evidence' or use bio-forensics to attribute confidently for a conviction on bioterrorism or bio-criminal activity. Nonetheless, the various counter terrorism

strategies discussed above point to ways threat actors may be disrupted on lesser offences while also providing a greater intelligence dividend on other individuals involved.

Cyber

The final knowledge area and stakeholder group that intelligence agencies and investigators working with bio-threat and risks may learn more from is cyber security. As Koblentz and Mazanec (2013) suggest there are a lot of common characteristics between biological and cyber weapons including but not limited to: difficulty of attribution and how multiple technologies can be used for offensive, defensive and civilian applications (421–425). Both authors argue because of these similarities there is likely a lot cyber can learn from how bio-threats have been managed historically. This is undoubtedly true, though in this section the focus will be the opposite—i.e. what can intelligence and investigative agencies working on bio-threats learn from the cyber threat and capability landscape? Even a cursory review of the literature suggest that there are a number of areas where current cyber research and practice could inform the 'Five Eyes' intelligence communities understanding of current and emerging bio-threats and risks. Space does not allow an exhaustive discussion on all of them, but there are three cyber areas in particular; where I believe those working with bio-threats and risks could benefit greatly from knowing more about in order to learn the lessons from the cyber context as well as identifying good intelligence and investigative practice. These areas are: the dark web, cyber terrorism and cyber espionage. I will discuss each briefly in turn.

Turning to the dark web environment first here we are referring to the content on the internet that is 'not indexed by standard search engines' (Weimann 2016: 196). Much of the dark web is hidden or blocked and can only be accessed by specialised browsers. Given the relative anonymity it provides, the dark web has seen the proliferation of child pornography, credit card fraud, identify theft, drugs and arms trafficking amongst other illicit offences. The dark web only emerged in recent years though law enforcement and intelligence agencies have

made some in roads into its penetration and disruption. The FBI's shut down of the dark web site Silk Road, which operated between February 2011 and October 2013 was to that point the largest and most sophisticated anonymous online market place for illicit drugs (Zajácz 2017). New technological solutions are also being developed to better identify, collect and analyse illicit activity on the dark web, including DARPA's MEMEX software, which helps catalogue dark web sites (Weimann 2016: 203). Nonetheless, all 'Five Eyes' intelligence communities will need to continue to develop their collection, analytical and investigative capabilities in the dark web content to profile more accurately various illicit market places in order to orchestrate impactful disruption activity across multiple markets.

Although it is unknown, at least in an unclassified sense the extent to which illicit markets exist that could benefit bio-threat actors (criminals or terrorists), undoubtedly law enforcement and intelligence agencies, who are given a watching brief on emerging bio-threats and risk should be exploiting the dark web more for opportunities for disruption. A first step might be first to map the bio-terrorism literature and identify researchers, who have access to bioterrorism agents/disease research, domain, institutions, countries and emerging topics and trends in bio-terrorism agents/disease research. Chen shows how by using informatics research it might be possible to use knowledge mapping techniques, to analyse productivity status, collaboration status and emerging topics in the bio-terrorism domain (Chen 2011: 335–367). Additionally, other intelligence and investigative teams that are working on non-bio threats such as conventional terrorist attacks, terrorism financing, drug trafficking or even child sexual exploitation may come across offenders, who have links to others interested in exploiting dual use biological agents for malevolent objectives. So the work currently going on by intelligence agencies working on broader cyber security issues such as cybercrime or cyber terrorism is directly relevant to improving collection and analysis against emerging bio-threats and risks.

Developments in the second area cyber-terrorism provides another opportunity for bio-threat intelligence and investigative teams to learn off their colleagues working on cyber threats. In the past we often think about the classical 'bio-terrorism' attack involving the aerolising and

dispersal of a dangerous pathogen like Anthrax into a crowded place. This mode of attack may still be chosen in the future by a terrorist group (leaving aside for a minute the technical difficulties of such an attack). Though committed acts through cyber opens up other choices for a bio-attack. Cyber security specialist's knowledge of cyber terrorism is still developing. We have seen for example groups like the Taliban and IS increasingly use computers for recruitment, propaganda and communications, but it remains difficult to know empirically how many of the current virtual attacks such as ransomware can be attributed to terrorist or led to deaths or impacted critical infrastructure in significant ways. Such attacks could just as easily be attributed to cyber hackers (criminals) or state sponsored espionage both issues we will return to shortly (Riglietti 2017; Bernard 2017; Heickerö 2014).

Nonetheless, it is clear that terrorism groups are increasing their use of computers including the dark web given they know that intelligence communities are monitoring the surface internet and social media. In August 2014, Al-Aan TV reported a laptop belonging to a Tunisian member of IS captured in Syria contained thousands of documents from the dark web including 19 pages about making biological weapons in a way to impact the biggest number of people (Weimann 2016: 200). There have also been cases where IS has carried out a series of cyber-attacks, 'exclusively computer based, which in one instance even led to the disclosure of private information regarding US government officials, from private conversations to work and email addresses' (Riglietti 2017: 19).

The final area of cyber security that is useful for bio-threat intelligence and investigative teams to reflect on relates to cyber hacks and espionage. Putting hacks and espionage together is not meant to suggest that both are always linked—though we have seen in the Russian interference in the 2016 US presidential election they can be. China too is playing an increasingly sophisticated and aggressive cyber espionage strategy aimed at political interference and stealing intellectual property (Inkster 2015). There seems little doubt that the extent of hacking (unauthorised access to a computer or network) being perpetrated by state and non-state actors is on the rise and network vulnerabilities across the civil and military space remain.

In a recent article, FBI Assistant Special Agent in Charge (Chicago), Todd Carroll said the average time between an unauthorised user getting inside a network and the user being detected is 150 days—'a lifetime in cyber means'. Todd went on to say that 57% of business owners don't have a dedicated employee or vendor monitoring for cyber-attacks (Stone 2017). We have also seen in recent years the growth in malware and ransomware attacks across the globe. For example, in 2017 the Wannacry ransomware attack caused 230,000 infections across 124 countries (locking down banking, energy and manufacturing systems) (Schilling 2017). The dark web also provides terrorist and criminal groups opportunities to operate botnet campaigns in anonymity that can remotely operate networks of computers to commit attacks on other systems including critical infrastructure. Again there is insufficient space to provide a full survey of all the cyber hacking and espionage threats, and indeed what to do about them is beyond the scope of this chapter (Clarke and Knake 2010: 257–280).

Nonetheless the hacking attacks—whether they are state sponsored (espionage) or non-state actors (terrorists or criminals) provide another rich source of knowledge to be collected and assessed that can be used by those working on emerging bio-threats and risks. For example, it would seem unwise for bio-threat intelligence and investigative teams to not learn from the fast changing angles of cyber-attack from hackers given how the physical security of biological institutions, their intellectual property and the kinds of biological products produced in such facilities is reliant on secure cyber systems. We have seen in recent years the take down of government websites involving ransomware attacks on both government and private sector networks. Increasingly more information is being shared and stored via the Cloud. What would be the impact of a major ransomware attack that locks down the entire bio-surveillance capability of a public health authority such as CDC do to maintaining national health security? Could a cybercriminal group infiltrate the network of a major biodefense company steal IP and sell it to a terrorist group on the dark web? Could research stored via the Cloud on non-secure networks relating to the genetic sequences of pathogens be stolen by a terrorist group or state actor to engineer bio-weapons? (Blue Ribbon Project 2015: 44–46). In all the three areas discussed above, a fuller

development of links between those working in the cyber intelligence collection and analysis streams, and those who might examine emerging bio-threats and risks is a necessary first step in bringing relevant knowledge and practice from cyber security to bio-threat stakeholders.

Treatment

In this final section the attention is turned to what kind of stakeholders play a role in treating bio-threats and risk? Second, in performing these roles, how can they help the 'Five Eyes' intelligence communities build better capability (knowledge, practice and technology) about treating actual or emerging bio-threats and risks? As we have seen so far the management of bio-threats and risks is potentially a crowded enterprise with many stakeholders (beyond the intelligence communities) playing critical roles. In this section, I have grouped them into three 'types of stakeholder': first responders, science and technology stakeholders and security stakeholders. These are not three distinct clusters of unique stakeholders that do not interact with each other. Depending on the nature of the bio-incident that has occurred, one would expect to see a close interaction amongst the various knowledge brokers and practitioners from each group. For example, a release of a synthetically manufactured select agent in an airport should result in the combined strategic and tactical contributions from first responders, engineers and security personnel rather each being delivered in isolation. An uncoordinated delivery of knowledge, practice and expertise to treat an unfolding bio-threat/risk from multiple stakeholders will not result in the best outcome for mitigating the risk or disrupting future potential of similar threats occurring.

Again as with previous sections, the focus here is not a deep exploration of the specific knowledge, practice or technology of all stakeholders involved potentially in the treatment of bio-risks. This would be an impossible task. Instead this section will explain briefly what each of the three broad stakeholder categories (first responders, science and technology and security) can do broadly to treat bio-risks (current or potential), what intelligence communities can learn from this in ways that extend their capabilities to manage bio-threats and risks.

First Responders

The label 'first responders' is a descriptor for a much broader range of stakeholders including: fire/hazmat, paramedics, emergency responders, health and hospital service providers. Each would play a different role in both responding to and treating a bio-incident depending on the type of biological hazard, their jurisdictional and legislative responsibilities and fiscal capacity. In all 'Five Eyes' countries with perhaps the exception of New Zealand (with a smaller population and only one national government) the complexity of response will be particularly governed by the overlapping roles that various local, state and federal first responders might play. Obviously in the US with multiple federal, state and local agencies, the coordination of first responder efforts to a bio-incident presents more challenges than other 'Five Eyes' countries such as Australia and the UK with less agencies and jurisdictions. There is not an abundance of academic literature on the role of first responders in treating bio-threats and risks. This lack of evidence makes it difficult to assess accurately what first responders can do to treat bio-threats and risks, what the challenges are and what the intelligence community can learn from these important stakeholders. There is however, some research available that can increase the intelligence communities' understanding of first responder capabilities to treat bio-threats and risks as well as illuminate some of the challenges in doing so. This research should provide at least a start to what the intelligence community can learn from first responders as they deploy their knowledge and practice to disrupt and treat bio-threats and risks.

9/11 and the *Amerithrax* incident provided a catalyst for law enforcement and public health agencies to work closer together to respond to an unfolding threat. Since *Amerithrax*, across the 'Five Eyes' countries further work has been done to better coordinate the work of law enforcement and public health agencies on treating bio-threats and risks. But such efforts have not involved routinely the broader spectrum of national security intelligence agencies, who have tended to play a more strategic and adhoc role compared to their law enforcement counterparts. Overall, policy, coordination and legislative efforts to bring first responders and members of the intelligence and law enforcement

community together have had only mixed success for a number of reasons. In 2007, a study of how law enforcement and public health agencies in the US, Canada, UK and Ireland work together on bio-threat incidents identified several common barriers to improving multi-agency responses (Strom and Eyerman 2007). These included cultural, legal, structural, communication and leadership barriers (ibid.: 135). Ten years on from Strom and Eyerman's research, other researchers have made similar observations about the ability of first responders to manage effectively a bio-threat incident and to work with law enforcement and intelligence community on such tasks. But it's not just the capability issues raised above, other research points to other technical challenges to treating the impact of bio-threats and risks in the physical environment. For example, research by chemists and environmental engineers show that given the varying nature and strains of the bacteria—the science for assessing risk of exposure may not be able to provide a fully accurate risk assessment of a building's vulnerability or resilience to a bio-attack nor—in some cases whether first responders have effectively 'cleaned the environment up after exposure' (Canter 2007; Taylor et al. 2013). A lack of effectiveness in responding to a bio-threat incident in a local area obviously can have broader public sector implications in both treatment and preparedness of bio-risks. For example, Gerstein (2017: 86) citing a study by advocacy group Trust for America's Health reported that 26 states and DC scored 6/10 or lower on a scale for preparedness. Additionally, since 9/11 major disease outbreaks such as SARS and Ebola have also demonstrated fragility in parts of the world, including some 'Five Eyes' country's public health response capability, which remains a concern if there was a major bio-terrorist event.

The Blue Ribbon Study Project Report raised similar concerns about the capability of certain responders including those local, state and federal agencies that might be involved in decontaminating sites following a bio-incident. In the US, the report raised similar coordination issues between federal, state and local agencies in which first responder agency would take the lead in decontaminating and remediating environments and how other agencies would get involved to ensure the attack site was deemed safe for people to return (Blue Ribbon Study

Project 2015: 26). One underlying theme arising from the studies mentioned on first responder's roles in treating bio-threats and risks is that the intelligence community must share more information with emergency services on the nature of the threat they are meant to respond to. This is not to suggest that in all the 'Five Eyes' countries that no sharing is going on. My selected interviews with law enforcement and intelligence officials in each country did not give the impression that no sharing was going on with first responders. However it is clear if the local fire officers or emergency staff in a hospital are meant to better respond to a bio-incident they will need regular, consistent, reliable, real-time information and intelligence. This is vital to them safely securing the scene, or rapidly diagnosing and treating infected patients while also keeping themselves safe. Importantly too, the more intelligence they receive will likely be helpful in first responders preserving any relevant evidence from the scene that might be needed by the either the law enforcement and intelligence communities. Gerstein makes a valuable point when referring to improving bio-preparedness and response activities, when he suggests that first responders need to be seen as part of a complex system rather than each representing a series of programs (Gerstein 2017: 88).

In addition to the range of knowledge and practice the intelligence community can learn from first responders, arguably the biggest lesson they can learn is to seek to better understand the 'linkages among disparate disciplines (biodefense, public health, emergency management), government, industry, the scientific community and themselves to better support first responders' (ibid.). If the 'Five Eyes' intelligence communities were able to create the necessary national health security coordination arrangements suggested in Chapter 6 such as the health security coordination council and the national health security strategy, then through these institutions further intelligence sharing mechanisms could be established to improve information flow between the intelligence communities and first responders at federal, state and local levels. However, first further research is required to investigate how law enforcement and intelligence communities work currently with first responders to identify and as much as possible ameliorate the cultural, legal, communication and leadership barriers that persist.

Science and Technology

A second cluster of knowledge and stakeholders for treating bio-threats and risks could be loosely described as 'science and technology' stakeholders. In earlier sections, under the relevant headings (prevention and disruption), significant space was devoted to how our intelligence communities can learn from a range of stakeholders working across a diverse array of disciplines (including bio-surveillance, public health, biosafety, criminology, counter terrorism and cyber). In each of these disciplines, discussion included exploration of relevant science, technology and knowledge useful for the intelligence community in preventing and disrupting bio-threats and risks. Some of that discussion, for example bio-surveillance, biosafety and strengthening global health is also relevant to our focus here in treating bio-incidents. However, in this section the focus is not what the intelligence community can learn from stakeholders working in the above disciplines, but rather what they can learn from disciplines more removed from the biological sciences or relevant social sciences (e.g. engineering or security studies).

What can the intelligence community learn from physical, mechanical or environmental engineering? There are multiple roles engineering specialties could play and are playing in preventing, disrupting and treating bio-threats and risks. For one and historically, the US DOD has relied on engineers, microbiologists to provide advice on weaponisation of biological agents under a range of scenarios and conditions (state actor and terrorists threats). For example, even pre 9/11, between 1999 and 2000 DTRA funded Project Bacchus to see if a team of scientists and engineers, who allegedly did not have extensive experience in bio-weapons could make bio-weapon facility using just commercially available items. The objective was to see if the team could make anthrax successfully without the detection of the intelligence community, though it was later revealed that this team did have substantive technical knowledge and support throughout this project (Vogel 2013: 41–43). Engineers have also long been engaged in studying aerolisation dynamics, which has become increasingly a multi-disciplinary collaboration of environmental engineers, biomedical engineers, microbiologists, chemists and epidemiologists (Xu et al. 2011). Related to aerolisation studies has been the

work of hardware and software engineers—many of whom came from the aerospace and automotive industries that have brought their skills into modelling bio-terrorism attacks to help first responders predict how airborne particles might move through sections of a city under certain weather and windflow conditions (Thilmany 2005).

Other engineering studies, sometimes referred to bio-protection studies have been important in the design of the heating ventilation and air conditioning (HVAC) systems used to resist biological contaminants. Much of this research became activated after the *Amerithrax* incident, and is designed at reducing the health consequences from airborne contaminants by augmenting heating and air conditioning systems (Ginsberg and Bui 2015). Another focus of engineering led research relates to improving the portability, speed and reliability of bio aerosol monitors for pathogens. One recent study has been working on a device that would be fully portable and automated—capable of detection of selected air-borne microorganisms on the spot—within 30 to 8 minutes depending on the genome and particular strain of the organism (Agranovski et al. 2017).

Security

In this last sub-section in our exploration of what other stakeholders may be useful in treating bio-threats and risks we turn our attention to the role of security officers. I am conscious in the discussion above regarding prevention and biosafety much was said about the role of security officers and managers in promoting biosecurity and biosafety across all sectors of the bio-sciences enterprise (e.g. research centres, hospitals, biotechnology companies, public and private labs). In this section, we focus instead on the role of security officers and managers across the broader economy—beyond biosciences. As argued in previous chapters, in addition to taking a one health perspective to bio-threats and risk, 'Five Eyes' intelligence communities and their law enforcement colleagues need to also understand the potential development of bio-threats and risks beyond the technical world of biotechnology and labs to include also in their wider social, economic and community contexts.

Hence in this section, we are referring to the role of security officers and companies that work across the international, national, state and local economies in each 'Five Eyes' country. Given the trajectory of most (if not all) future bio-threats is unknown, our intelligence communities need to be forging more formalised (less adhoc) relationships with security officers in a range of non-biotechnology industries (banking, mining, food supply, agriculture, critical infrastructure).

As Nalla and Wakefield (2014) argue several factors have increased the role of private security since the Second World War. Increased economic wealth, enhanced security technology (alarms, access control and CCTV), in addition to an increase in the control by a number of private sector companies of publicly accessible places have, amongst other factors all contributed to the growth in private sector security (ibid.: 727). While it is difficult to generalise 'as the functions of security officers/agencies are as varied as the organisations that employ them' (ibid.: 731), their functions and roles cut across many facets of each 'Five Eyes' nation to include office buildings, warehouses, shopping malls, education establishments, residential complexes and critical infrastructure. One often thinks of the classic scenario of a security guard standing in front of a physical gate, which is one role of many others which might also, depending on their functions include traffic control, surveillance, responding to emergencies, security vetting. In the security role of complex large companies, airports and electricity plants, it is likely that the security officers will have a deep understanding of their physical and virtual security environments and this kind of expert knowledge would be integral for them and the intelligence community gaining threat awareness, prevention, surveillance, disruption, treatment and recovery to bio threats and risks which may manifest in their operating environment.

Historically however, the relationship between intelligence communities (including law enforcement) and private sector security has not been optimal partially because a lack of trust between both (ibid.: 739). However, several studies on private and public sector security do show several areas of improvement across each 'Five Eyes' country. Some of these improvements have been initiated by governments such as in the UK making significant cuts to policing in the late 1990s and mid-2000s

and seeking the private sector security sector to pick up more cheaply what were considered less core policing such as offender management and transfers of prisoners. In other cases, governments were interested in engaging with the private sector to extend their own security and intelligence collection capabilities with terrorism. Connors et al. (2000), Wakefield (2003), and Rigakos (2002) provide more detailed analysis of a range of factors that have been involved in building partnerships with private sector security companies in the US, UK and Canada respectively. 9/11 and of course subsequent terrorist attacks in many western countries has seen a more focused attempt by 'Five Eyes' countries to reach out to the private sector—including private sector security given many attacks occur in public places owned or managed by the private sector. Threats as well to public and privately owned critical infrastructure (aviation, power, water, and telecommunication) have also influenced 'Five Eyes' government's closer liaison with the private sector. For example in the US, DHS has established a private sector office to provide government advice on relevant security issues to the private sector as well as promoting public-private partnerships. In Australia, since 9/11 parts of the Australian intelligence community, particularly ASIO has developed closer links with the private sector. In 2004 Australia's Attorney General's Department created the Business-Government Advisory Group on National Security to provide a vehicle for the Government to discuss a range of national security issues and initiative with CEOs and senior business leaders (DPM &C 2015: 6). The group later (2014) evolved into the Australian Governments Industry Consultation on National Security (ibid.).

More recently (2017) the Australian Government released its strategy for protecting crowded places from terrorism. This significant policy document was developed in close partnerships with federal, state and local governments, the intelligence community and the private sector. The key objective being to assist owners and operators to increase the safety, protection and resilience of crowded places across Australia (ANZCTC 2017). An interesting aspect of this strategy is that it places the primary responsibility for protecting sites and people on private sector businesses. Similar policy articulations have been declared in the UK's counter-terrorism strategy (HMG 2011) and Canada's approach to counter-terrorism (Canadian Government 2011).

In summary, it's clear that various agencies of the 'Five Eyes' intelligence communities and their broader law enforcement counterparts have increased their liaison and implemented various initiatives with private sector industry. What is less clear is the nature and extent of these as they relate to the prevention, disruption and treatment of potential bio-threats and risks. Much is unknown, for example, about whether intelligence and law enforcement communities are actively working in partnership with the private sector beyond the classical threat typologies of basic terrorist's tactics, improvised explosive devices or vehicle born attacks. Given the low probability high impact nature of the evolving bio-threat environment, it is likely that many private sector companies (banking, shopping malls, mining, hotels) see little need to include bio-threats in their security risk management plans or indeed consult with intelligence and law enforcement communities on them.

While it is important not to be alarmist on low probability threats that are more likely on balance to effect the biosciences community rather than the broader private sector economy, it seems unwise for the latter not to consider the impact of such bio-threats on their operations and to at least have formalised dialogues on these with the intelligence community. But such a dialogue will in the future rely on several factors identified already by researchers coming together to develop more effective public-private crime prevention strategies. Prenzler and Sarre list several factors including: a common interest in reducing a specific crime, leadership, mutual respect, information sharing based on high levels of trust in confidentiality and formalised mechanisms for consultation and communications (Prenzler and Sarre 2014: 783).

Conclusion

This chapter surveyed the role of external stakeholders external (to the 'Five Eyes' intelligence communities) in preventing, disrupting and treating bio-threats and risks. Depending on the particular bio-threat a diverse array of stakeholders could provide knowledge, skills and capabilities to the intelligence community. The large number of disciplines

and stakeholders with relevant technical knowledge suggest that they will continue to play a critical role in the prevention, disruption and treatment of bio-threats and risks. In many cases, such as in bio-surveillance, forensics and even engineering the scientific and technical stakeholders discussed here may play a greater role than the traditional intelligence and investigative response to managing bio-threats and risks.

The chapter also highlighted that although each 'Five Eye's intelligence community has a wealth of knowledge to tap into from stakeholders, however in most cases all stakeholder groups are faced with their own theoretical and practical limitations. Analysts and investigators working on bio-threats and risks need to understand these limitations while also seeking to build deeper and more formalised partnerships with scientific, technical and cross disciplinary stakeholders. In the final Chapter 8, we shift the focus away from the practice and processes involved in interpreting bio-threats and risks to oversight and accountability issues. Given the legislative, ethical and normative challenges modern intelligence practice faces, particularly in understanding the potential threat trajectory of synthetic biology, what role can oversight and accountability play in achieving the objectives of the intelligence communities in liberal democracies?

References

Agranovski, I. E., et al. (2017). Miniature PCR Based Portable Bioaerosol Monitor Development. *Journal of Applied Microbiology, 122*(1), 129–138. https://doi.org/10.1111/jam.13318.

ANZCTC, (2017). *Australia's Strategy for Protecting Crowded Places from Terrorism*. ANZCTC, Australian Government.

Australia Group. (2015). *Common Control List Handbook, Volume 2: Biological Weapons-Related Common Control Lists*. From www.defence.gov.au/export-controls/master/docs/AustGroupCommonControlListHandbaookVolIIpdf. Accessed March 12, 2017.

Bakanidze, L., et al. (2010). Biosafety and Biosecurity as Essential Pillars of International Health Security and Cross-Cutting Elements of Biological Non-Proliferation. *Biomed Central, 10*, 1–8.

Berger, K. (2013). Biosecurity in Research Laboratories. In R. Burnette (Ed.), *Biosecurity* (pp. 113–128). Hoboken, NJ: Wiley.

Bernard, R. (2017). These Are Not the Terrorist Groups You're Looking for: An Assessment of the Cyber Capabilities of Islamic State. *Journal of Cyber Policy, 2*(2), 255–265. https://doi.org/10.1080/23738871.2017.1334805.

Blue Ribbon Study Panel. (2015). *Blue Ribbon Study Panel on Biodefense. A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimise Efforts*. Washington, DC: Hudson Institute for Policy Studies.

Blue Ribbon Study Panel. (2017). *Biodefense Special Focus: Defense of Animal Agriculture*. Washington, DC: Blue Ribbon Study Panel.

Buehler, J., et al. (2004). Group CDCW. Framework for Evaluating Public Health Surveillance Systems for Early Detection of Outbreaks: Recommendations from the CDC Working Group. *MMWR Recommendations and Reports: Morbidity and Mortality Weekly Report, 53,* 1–11.

Bunn, M., & Sagan, S. (Eds.). (2016). *Insider Threats*. Ithaca, NY: Cornell University Press.

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

BWC. (2017). *BWC Newsletter*. Geneva: United Nations.

Canadian Government. (2011). *Building Resilience Against Terrorism: Canada's Counter Terrorism Strategy*. Ottawa: Government of Canada.

Cameron, E. (2017, July 19). Biosecurity Imperative: An Urgent Case for Extending the Global Health Security Agenda. *Atomic Pulse*.

Canter, D. (2007). Addressing Residual Risk Issues at Anthrax Clean Up. How Clean Is Safe? *Journal of Toxicology and Environmental Health, Part A, 68*(11–12), 1017–1032.

CDC. (2014). *Report on the Potential Exposure to Anthrax*. Atlanta, GA: CDC.

CDC. (2015a). *90 Day Internal Review of the Division of Select Agents and Toxins*. Atlanta, GA: CDC.

CDC. (2015b). Report of the Advisory Committee to the Director, CDC Follow Up on CDC Progress.

Chen, H. (2011). *Bioterrorism and Knowledge Mapping Dark Web Exploring and Data Mining the Dark Side of the Web* (pp. 335–367). New York, NY: Springer.

Chevrier, M., & Spelling, A. (2016). The Traditional Tools of Biological Arms Control and Disarmament. In F. Lentzos (Ed.), *Biological Threats in the 21st Century* (pp. 331–356). London: Imperial College Press.

Clarke, R., & Knake, R. (2010). *Cyber War*. New York, NY: Ecco.

Collier, N. (2015). A Review of Web-Based Epidemic Detection. In S. Davies & J. Youde (Eds.), *The Politics of Surveillance and Response to Disease Outbreaks* (pp. 85–107). Surrey, UK: Ashgate.

Connors, E., et al. (2000). *Operation Cooperation, Guidelines for Partnerships Between Law Enforcement and Private Security Organisations*. Rockville, MD: Bureau of Justice Assistance.

Danzell, O., & Montanez, L. (2016). Understanding the Lone Wolf Phenomena: Assessing Current Profiles. *Behavioural Sciences of Terrorism and Political Aggression, 8*(2), 135–159.

Dennis, B., & Sun, L. (2014a, July 16). FDA Found More Than Smallpox Vials in Storage Room. *Washington Post*. From https://www.washingtonpost.com/national/health-science/fda-found-more-than-smallpox-vials-in-storage-room/2014/07/16/850d4b12-0d22-11e4-8341-b8072b1e7348_story.html?utm_term=.978241b9d1f8. Accessed March 14, 2017.

Dennis, B., & Sun, L. (2014b, September 5). More Deadly Pathogens, Toxins Found Improperly Stored in NIH and FDA Labs. *Washington Post*. From https://www.washingtonpost.com/national/health-science/six-more-deadly-pathogens-found-improperly-stored-in-nih-and-fda-labs/2014/09/05/9ff8c3c2-3520-11e4-a723-fa3895a25d02_story.html?utm_term=.4bc6ce160f62. Accessed March 14, 2017.

Dickmann, P., et al. (2015). Marburg Biosafety and Biosecurity Scale (MBBS): A Framework for Risk Assessment and Risk Communication. *Health Security, 13*(2), 88–95. https://doi.org/10.1089/hrs.2014.0065.

DPM &C. (2015). *Review of Australia's Counter Terrorism Machinery*. Department of Prime Minister and Cabinet, Australian Government.

Dzau, V., & Sands, P. (2016). Beyond the Ebola Battle Winning the War Against Future Epidemics. *New England Journal of Medicine, 375,* 203–204.

Eaves, E. (2017). IARPA Director Jason Matheny Advances Tech Tools for US Espionage. *Bulletin of the Atomic Scientists, 73*(2), 67–73.

GAO. (2009). *High Containment Laboratories: National Strategy for Oversight is Needed*. Washington, DC: GAO.

GAO. (2011). *Biosurveillance Non Federal Capabilities Should Be Considered in Creating a National Biosurveillance Strategy*. Washington, DC: GAO.

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).

GAO. (2016). *Testimony Before the Subcommittee on Emergency Preparedness Response and Communications, Committee on Homeland Security, House of Representatives*. Washington, DC: GAO.

GAO. (2017). *GAO High Containment Labs Coordinated Actions Needed to Enhance the Select Agent Program's Oversight of Hazardous Pathogens* (Vol. GAO 18–145). Washington, DC: GAO.

Geoghegan, J., & Holmes, E. (2017). Predicting Virus Emergencies and Evolutionary Noise. *Open Biology, 7,* 1–9.

Gerstein, D. (2013). *The Biological and Toxin Weapons Convention. National Security and Arms Control in the Age of Biotechnology*. Lanham, MD: Rowman and Littlefield.

Gerstein, G. (2017). Glaring Gaps: America Needs a Biodefense Upgrade. *Bulletin of the Atomic Scientists, 73*(2), 86–91.

GHRF Commission. (2015). *The Neglected Dimension of Global Security. A Framework to Counter Infectious Disease Crisis*. Washington, DC: Global Health Risk Framework for the Future Commission.

Ginsberg, M., & Bui, A. (2015). Bio Protection of Facilities. *Defense & Security Analysis, 31*(1), 4–21. https://doi.org/10.1080/14751798.2014.995335.

Gronvall, G., et al. (2016). National Biosafety Systems. UPMC Center for Health Security.

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

Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. *Strategic Analysis, 38*(4), 554–565. https://doi.org/10.1080/09700161.2014.918435.

Heymann, D., et al. (2015). Global Health Security: The Wider Lessons from the West African Ebola Virus Disease Outbreak. *The Lancet, 385*, 1884–1901.

HMG. (2011). *CONTEST: The UK's Strategy for Countering Terrorism*. London: Her Majesty's Government.

Inkster, N. (2015). Cyber Espionage. *Adelphi Series, 55*(456), 51–82. https://doi.org/10.1080/19445571.2015.1181443.

Innes, M., & Sheptycki, J. (2004). From Detection to Disruption: Intelligence and the Changing Logic of Police Crime Control in the UK. *International Criminal Justice Review, 14,* 1–24.

Innes, M., et al. (2017). A Disruptive Influence? Preventing Problems and Counter Violent Extremism Policy in Practice. *Law and Society Review, 51*(2), 252–281.

Insinna, V. (2013). Government Biosurveillance to Include Social Media. *National Defense, 97*(710), 13.

Kasolo, F., et al. (2013). Implementation of the International Health Regulations (2015) in the African Region. *African Health Monitor, 18,* 11–13.

Kim, J., et al. (2015). Advances in Anthrax Detection: Overview of Bioprobes and Biosensors. *Applied Biochemistry and Biotechnology, 176*(4), 957–977.
Koblentz, G. (2009). *Living Weapons*. New York: Cornell University Press.
Koblentz, G., & Mazanec, B. (2013). Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy, 32*(5), 418–434. https://doi.org/10.1080/01495933.2013.821845.
Lennane, R. (2011). Biological Weapon Convention. In R. Katz & R. Zilinskas (Eds.), *Encyclopaedia of Bioterrorism Defense* (pp. 82–86). Hoboken, NJ: Wiley-Blackwell.
Marston, B., et al. (2017). Ebola Response Impact on Public Health Programs, West Africa 2014–2017. *Emerging Infectious Diseases Journal, 28*(Supplement), 25–31.
Mawudeku, A., et al. (2015). GPHIN Phase 3: One Mandate, Multiple Stakeholders. In S. Davies & J. Youde (Eds.), *The Politics of Surveillance and Response to Disease Outbreaks* (pp. 71–85). Surrey, UK: Ashgate.
MMWR. (2016). CDC's Response to the 2014–2016 Ebola Epidemic West Africa and the United States. *MMWR, Supplement, 65*(3), 1–106.
Nalla M.K., & Wakefield A. (2014). The Security Officer. In M. Gill (Ed.), *The Handbook of Security* (pp. 727–746). London: Palgrave Macmillan.
National Institute for Public Policy. (2009). The Proliferation Security Initiative: A Model for Future International Collaboration. *Comparative Strategy, 28,* 395–462.
Nature Editorial. (2014). Biosafety in the Balance. *Nature, 510*, 443.
O'Shea, J. (2017). Digital Disease Detection: A Systematic Review of Event-Based Internet Biosurveillance Systems. *International Journal of Medical Informatics, 101*(Supplement C), 15–22. https://doi.org/10.1016/j.ijmedinf.2017.01.019.
Paranjape, S., & Franz, D. (2015). Implementing the Global Health Security Agenda Lessons from the Global Health and Security Programs. *Health Security, 13*(1), 9–19.
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.
Prenzler, T., & Sarre, R. (2014). The Role of Partnerships Security Management. In M. Gill (Ed.), *The Handbook of Security* (pp. 791–812). Basingstoke: Palgrave Macmillan.
Ratcliffe, J. (2008). *Intelligence Led Policing*. Collompton, UK: Willan.
Ratcliffe, J. (2016). *Intelligence Led Policing* (2nd ed.). Abingdon, UK: Routledge.
Reed, M. (2016). *The Research Impact Handbook*. Huntly, UK: Fast Track Impact Ltd.

Regalado, A. (2016, February 9). Top US Intel Official Calls Gene Editing a WMD Threat. *MIT Technology Review*.

Rigakos, G. (2002). *The Para Police*. Toronto: University of Toronto Press.

Riglietti, G. (2017). Defining the Threat: What Cyber Terrorism Means Today and What It Could Mean Tomorrow. *International Journal of Business and Cyber Security, 1*(2).

Robert Koch Institute. (2018). *Signale—Early Warning System*. Berlin: Robert Koch Institute. From https://www.rki.de/EN/Content/infections/epidemiology/signals/signals_node.html. Accessed March 15, 2018.

Salerno, R., & Gaudioso, J. (Eds.). (2015). *Laboratory Biorisk Management Biosafety and Biosecurity*. Boca Raton, FL: CRC Press.

Sample, I. (2014). Revealed: 100 Safety Breaches at UK Labs Handling Potentially Deadly Diseases. *The Guardian*. From https://www.theguardian.com/science/2014/dec/04/-sp-100-safety-breaches-uk-labs-potentially-deadly-diseases. Accessed March 15, 2017.

Schilling, J. (2017). Ransomware101-How to Face the Threat. *Petroleum Accounting and Financial Management Journal, 36*(2), 6–8.

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.

Schnirring, L. (2016, January 13). Pandemic Readiness Review Says $4.5 Billion a Year Needed. *CIDRAP*. From http://www.cidrap.umn.edu/news-perspective/2016/01/pandemic-readiness-review-says-45-billion-year-needed. Accessed March 15, 2017.

Schnirring, L. (2017). Secretary Tillerson Lauds Global Health Security Agenda. Minneapolis, MN: University of Minnesota (CIDRAP). Retrieved from http://www.cidrap.umn.edu/news-perspective/2017/10/secretary-tillerson-lauds-global-health-security-agenda.

Shaikh, A.T., Ferland, L., Hood-Cree, R., Shaffer, L., & McNabb, S. (2015). Disruptive Innovation Can Prevent the Next Pandemic. *Frontiers in Public Health, 3*(215). https://doi.org/10.3389/fpubh.2015.00215.

Shinwari, Z., Khalil, A., & Nasim, A. (2014). Natural or Deliberate Outbreak in Pakistan: How to Prevent or Detect and Trace Its Origin: Biosecurity, Surveillance Forensics. *Archivum Immunologiae et Therapiae Experimentalis, 62*(4), 263–275. https://doi.org/10.1007/s00005-014-0298-6.

Sisk, R. (2016). Army Probe of Anthrax Scandal Raises More Red Flags. *Military.Com*. Retrieved from http://www.military.com/daily-news/2016/01/13/army-probe-of-anthrax-scandal-raises-more-red-flags.html.

Slayton, J., et al. (2013). Physical Elements of Biosecurity. In R. Burnette (Ed.), *Biosecurity* (pp. 51–70). Hoboken, NJ: Wiley.

Sparrow, A. (2016). Who Isn't Equipped for a Pandemic or Bioterror Attack? The WHO. *Bulletin of the Atomic Scientists*. From https://thebulletin.org/who-isnt-equipped-pandemic-or-bioterror-attack-who9555. Accessed March 15, 2017.

Stern, J., & Shouten, R. (2016). Lessons from the Anthrax Letters. In M. Dunn & S. Sagan (Eds.), *Insider Threats* (pp. 74–102). Ithaca and New York: Cornell University Press.

Stone, R. (2017). *The Week in Fintech: FBI Agent Says Cybersecurity Practices Need to Change*. New York: SNL Financial LC.

Strom, K., & Eyerman, J. (2007). Interagency Coordination in Response to Terrorism: Promising Practices and Barriers Identified in Four Countries. *Criminal Justice Studies, 20*(2), 131–147. https://doi.org/10.1080/14786010701396871.

Sture, J., Minehata, M., & Shinomiya, N. (2012). Looking at the Formulation of National Biosecurity Education Action Plans. *Medicine, Conflict and Survival, 28*(1), 85–97. https://doi.org/10.1080/13623699.2012.658628.

Taylor, J., et al. (2013). The Role of Protection Measures and their Interaction in Determining Building Vulnerability and Resilience to Bioterrorism. *Bioterrorism and Biodefense, 4*(1), 1–10.

Thilmany, J. (2005). Harms Way Engineering Software and Micro Technology Prepare the Defense Against Bioterrorism. *Mechanical Engineering CIME, 127*(8), 22–25.

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

Wakefield, A. (2003). *Selling Security. The Private Policing of Public Space*. Cullompton and Devon: Willan.

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

Walsh, P. F. (2016). Australian National Security Intelligence Collection Since 9/11: Policy and Legislative Challenges. In K. Warby (Ed.), *National Security, Surveillance and Terror* (pp. 51–74). Cham, Switzerland: Springer International Publishing.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism, 39*(3), 195–206. https://doi.org/10.1080/1057610X.2015.1119546.

WHO. (2015). Ebola Virus Disease in West Africa—The First Nine Months of the Epidemic and Forward Projections. *The New England Journal of Medicine, 371,* 1481–1495.

Wilson, J. (2017). Signal Recognition During the Emergence of Pandemic Influenza Type A/H1N1: A Commercial Disease Intelligence Unit's Perspective. *Intelligence and National Security, 32*(2), 222–230.

Xu, Z., et al. (2011). Bioaerosol Science, Technology and Engineering: Past and Present. *Aerosol Science and Technology, 45*(1), 1337–1349.

Yan, S., et al. (2017). Utility and Potential of Rapid Epidemic Intelligence from Internet-Based Sources. *International Journal of Infectious Diseases, 63*(Supplement C), 77–87. https://doi.org/10.1016/j.ijid.2017.07.020.

Young, A. (2015, August 28). Labs Cited for 'Serious' Security Failures in Research with Bioterror Germs. *USA Today*. From http://www.usatoday.com/story/news/2015/08/28/lab-security-violation-bioterrorism-select-agent-regulation/32439491/. Accessed March 15, 2017.

Zajácz, R. (2017). Silk Road: The Market Beyond the Reach of the State. *The Information Society, 33*(1), 23–34. https://doi.org/10.1080/01972243.2016.1248612.