The London School of Economics and Political Science

Governing through risk

Synthetic biology and the risk management process

R. Alexander Hamilton

A thesis submitted to the Department of Sociology of the London School of Economics for the degree of Doctor of Philosophy

Declaration

I certify that the thesis I have presented for examination for the MPhil/PhD degree of the London School of Economics and Political Science is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it).

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

I declare that my thesis consists of 105,388 words.

Abstract

In recent years, synthetic biology – an emerging science that promises to 'democratize' bioengineering – has emerged as a key site of regulatory interest and concern. In the United States, in particular, these concerns have largely been voiced in relation to synthetic biology's perceived capacity to enable an act of bioterrorism. This thesis examines the regulatory response – a 'risk management process' – that has been mounted to address this contingency, and which seeks to 'secure' and 'sustain' a science characterized by sharply contrasting expectations.

In particular, this thesis engages with the discursive and non-discursive practices enacted by diverse scientific and technical experts determined to assess and manage 'risks' that threaten to exceed the very capacity of risk, as a 'calculative rationality', to tame chance and legitimize responsible action. Yet, in the face of uncertainty, and in stark contrast to the 'risk society' thesis, this thesis underlines that uncertainty is not an inhibition to risk management, but a call for more intensive and more creative ways of organizing uncertainty, enabling action in the present. Indeed, in the case of regulating synthetic biology, risk management is, above all, tailored to finding practical 'solutions' to seemingly intractable policy 'problems'.

In addition to its contribution to recent scholarship that has drawn on Foucault's concept of 'governmentality' to examine how diverse social problems, ranging from climate change to terrorism, are 'governed through risk', this thesis critically examines how biotechnology's pairing with the perceived threat of bioterrorism is influencing the manner in which modern biology is understood, represented, practiced and controlled. Thus, the case of synthetic biology examined in this thesis not only provides a lens through which to advance risk theory in sociology, but also serves as a vector through which to explore changing configurations of 'risk' and 'risk responsibility' in the contemporary life sciences.

Acknowledgments

I would like to thank my advisors, Filippa Lentzos and Nikolas Rose, for their guidance and support during the course of my PhD. They have helped me navigate a research process that has been both challenging and immensely rewarding. From the outset of my PhD, I was encouraged to be patient, to read widely, to choose a research topic of particular interest, and to develop my own 'voice' through a research process beginning with the conception of a research idea and concluding with a thesis developed over the course of four years.

I am especially grateful to Nikolas Rose for his theoretical insights and enthusiasm for the production of new knowledge in a field he knows so well. And, I will always be grateful to Filippa Lentzos for encouraging me to pursue my PhD and for inviting me to participate as an observer at the Biological Weapons Convention. Her thoughtful introductions and guidance enabled me gain access to numerous opportunities that have enhanced my education and research.

To the experts interviewed for my research, who I have had the privilege to get to know during my field research at the Biological Weapons Convention, I am grateful for both their time and their willingness to speak openly about their work, and about the challenges and opportunities faced by policymakers and regulators seeking to ensure the security and sustainability of biotechnology.

Finally, to the LSE and Canada's Social Science and Humanities Research Council, I am grateful for the financial support that has made this PhD possible.

Acronyms and abbreviated titles

BWC	Biological Weapons Convention
CDC	Centers for Disease Control and Prevention
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DIYbio	Do-it-yourself biology
FBI	Federal Bureau of Investigation
Fink Report	Biotechnology Research in an age of terrorism: Confronting the dual use dilemma
IBC	Institutional biosafety committee
iGEM Competition	International Genetically Engineered Machine Competition
MIT	Massachusetts Institute of Technology
NAS	National Academy of Sciences
NIH	National Institutes of Health
NRC	National Research Council
NSABB	National Science Advisory Board for Biosecurity
NSDD-189	National Security Decision Directive 189
PCSBI	Presidential Commission for the Study of Bioethical Issues
Screening Framework	Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA
UNICRI	United Nations Interregional Crime and Justice Research Institute
USAMRIID	US Army Medical Research Institute of Infectious Diseases
WHO	World Health Organization
WMD	Weapons of Mass Destruction

List of Figures and Tables

Table of Contents

1. Introduction

1.1 Synthetic biology

Described as "another transformative innovation", synthetic biology promises to be the next generation of 'genetic engineering', one "that will make it possible to build living machines from off-the-shelf chemical ingredients" (Tucker and Zilinskas 2006, p. 25). A distinctly reductionist view of biology, the science is grounded in the belief that it is possible to transition from ideas for biological 'things' – proteins, genomes or (micro)organisms – to the genetic sequence information that describes those things – a series of A's, T's, G's and C's representing the four nucleotides that comprise DNA – and from genetic sequence information to the things themselves. In brief, synthetic biology suggests the possibility of designing and constructing life 'from scratch' (Rasmussen et al. 2004; Garfinkel et al. 2007). According to its most outspoken advocates – the scientists who are presently imagining synthetic biology's methodologies, vocabularies and assorted techniques – the aim is to make biology 'simple to engineer' (Endy 2005), enabling scientists, and in time 'anyone' with an innovative idea for a biological application, to design and build novel biological entities that can be applied to all sorts of societal needs.

Emerging as a more or less coherent 'field' only within the last ten years (Balmer and Martin 2008), synthetic biology (as a science and a source of seemingly boundless expectations) is still very much in the process of being imagined. At the forefront of this process, a number of pioneering 'synthetic biologists'[1] seek to differentiate a new domain of biotechnology, setting their science apart from 'traditional' approaches to genetic engineering. In particular, it is with a view to the increased productivity and rapidly falling cost of automated DNA sequencing and synthesis (Carlson 2008) that synthetic biologists claim an enhanced capacity to 'read' (DNA sequencing) and 'write' (DNA synthesis) the so-called "building blocks

[1] See de Vriend (2006, pp. 41-44) for an overview of some of the "[k]ey players in the scientific community" (ibid, p. 41) who have been instrumental in establishing the 'field' of synthetic biology, including Drew Endy (interviewed for my research).

of life" (deoxyribonucleic acid or 'DNA') (Garfinkel et al. 2007, p. 5). In the first instance, advances in DNA sequencing technology are credited with enabling the identification of the complete genome sequences of numerous organisms, providing a growing repository of genetic sequence information that is freely accessible online (NSABB 2006, 2010). In the second instance, and of particular importance to the realization of synthetic biologists' engineering goals, advances in DNA synthesis technology are credited with permitting increasingly large strands of DNA to be 'printed' from raw chemicals and digital sequence information, enabling the construction of bespoke biological entities, ranging from single genes to complete genomes (Bügl et al. 2007; Garfinkel et al. 2007, 2008; Carlson 2008).

Underpinning an approach to synthetic biology known as 'synthetic genomics' (Garfinkel et al. 2007, 2008), advances in these so-called 'foundational technologies' (Endy 2005) represent the cornerstones of a science that seeks to make the project of engineering life a realizable, if not practical, goal. Indeed, in light of advances in DNA synthesis (an activity increasingly outsourced to companies specializing in gene- to genome-length 'synthetic DNA'),[2] as the authors of one prominent report on synthetic genomics assert, "we take as a given that now, or within a few years, any virus with a known sequence can or will be able to be constructed in a relatively straightforward manner" (Garfinkel et al. 2007, p. 15). The expectation being, 'synthetic microorganisms' of this kind can be used as a platform for the production of various "bio-based products", ranging from biofuels to new vaccines and pharmaceuticals (ibid, p. 10). Moreover, and of no less significance, continued advances in synthetic genomics are not only anticipated to make it increasingly feasible to reproduce known biological entities, but also to

[2] In this context, the term 'synthetic' does not necessarily mean that 'synthetic DNA' is structurally or chemically different than its naturally occurring counterpart (although some branches of synthetic biology are investigating 'novel nucleotides'). Rather, it more precisely refers to the process used to assemble DNA. That is, it refers to DNA that is chemically synthesized and assembled using a 'DNA synthesizer' (a piece of laboratory equipment) as opposed to DNA produced through normal cell division. In the scientific and technical literature, this is sometimes referred to as 'synthetically derived' as opposed to 'naturally derived' DNA (see, for example, NSABB 2006, p. 4).

produce new ones – genetic constructs and forms of life that are not simply 'replicated' or 'modified' but '*created*' through the *de novo* synthesis of "any specified DNA sequence" (ibid, p. 6). From this perspective, in contrast to genetic engineering (or 'recombinant DNA') techniques developed in the 1970s, which rely on the transfer of individual genes between organisms, synthetic genomics could provide a pathway to entirely new forms of biological diversity.

In addition to claiming an enhanced capacity to carry out the *de novo* synthesis of genes and genomes using DNA synthesis technology and 'off-the-shelf' chemicals, synthetic biologists aspire for a more intuitive, rational biology that will enable more people to engage in advanced bioengineering work. At the heart of these claims is the so-called 'parts-based' approach to synthetic biology (Benner and Sismour 2005; Endy 2005; Purnick and Weiss 2009). Under this approach, synthetic biologists strive to produce 'standard biological parts' (characterized sequences of DNA that 'code' for specific proteins or basic biological functions) and 'genetic circuits' (multiple 'parts' linked together to produce specific biological processes that control cellular behavior), akin to the transistors and circuits familiar to electrical engineers (ibid.). A distinct (and widely publicized) feature of synthetic biology, standard biological parts (commonly known as 'BioBricks')[3] embody the engineering aspirations of synthetic biologists and the promise of a science that could enable the construction of bespoke biological systems in much the same way Lego blocks are assembled to produce various three-dimensional structures. Referred to by some commentators as the "legoization" of biology (Nature Biotechnology 2009, p. 1073), "[t]he end goal is to create a catalogue of interchangeable parts that can be easily mixed and matched for circuit construction" (Purnick and Weiss 2009, p. 411), enabling the predicable modification of naturally occurring organisms or the construction of novel biological systems.

In sum, 'synthetic biology' tends to be differentiated from earlier attempts at genetic engineering on the basis of advances in 'foundational technologies' and on the basis of a 'parts-based' approach to the design and assembly of 'genetic circuits'.

[3] See 'BioBricks Foundation', which describes 'BioBricks' as "the fundamental building blocks of synthetic biology" (http://biobricks.org/about-foundation/).

If not singularly 'new', it is nonetheless widely agreed that synthetic biology "marks the maturity of a series of powerful technologies" and a "growing confidence in the scientific community to undertake the project of engineering life" (Balmer and Martin 2008, p. 29). Significantly, these (rhetorical) features of the science bring with them not only a new vision for how modern biology can be conducted – one that suggests the possibility of a biology that is 'simple to engineer' (Endy 2005) – but also an open-ended set of expectations (Kwok 2010). That is, if biology is no longer constrained by 'natural' genetic sequences; if 'novel' genetic constructs, genomes and microorganisms need only be imagined and then produced using readily accessible technologies, then "the possibilities of synthetic … biological structures and systems seem endless" (de Vriend 2006, p. 29). Following this logic, synthetic biology suggests numerous applications, including:

> "[T]he creation of bioengineered microorganisms (and possibly other life forms) that can produce pharmaceuticals, detect toxic chemicals, break down pollutants, repair defective genes, destroy cancer cells, and generate hydrogen for the postpetroleum economy." (Tucker and Zilinskas 2006, p. 25)

In brief, as one news feature in the scientific journal *Nature* observed in 2010: "To read some accounts of synthetic biology, the ability to manipulate life seems restricted only by the imagination" (Kwok 2010, p. 288).

1.2 Synthetic biologists

At the same time that synthetic biology, as a 'field', is being defined, so, too, is the very notion of a 'synthetic biologist'. Prior to the widespread use of the term 'synthetic biology' in the mid-2000s (Balmer and Martin 2008), synthetic biologists went by other professional titles. Notably, synthetic biology's early practitioners were predominately "natural scientists and technologists from different disciplines, most of them based in the USA" (de Vriend 2006, p. 65) who shared a common interest in testing the hypothesis, 'could biology be made simple to engineer' (Endy 2005)? Representing prestigious "universities and institutes such as the Massachusetts Institute of Technology (MIT), the California Institute of Technology

(CalTech), the Lawrence Berkeley National Laboratory, the J. Craig Venter Institute, and the Harvard Medical School" (de Vriend 2006, p. 65), these individuals played an instrumental role in establishing the aims and methods of synthetic biology, generating support for a wider 'synthetic biology movement'. As Bauer and Gaskell (2002) observe in relation to the 'biotechnology movement' more generally, the claims and evocations of pioneering synthetic biologists (as advocates for a new approach to biological engineering) played a vital role in the symbolic elaboration of the science, as well as influencing expectations for the future of the field.

Today, "traditional life scientists as well as engineers, chemists, materials scientists, computer modelers and others" (NSABB 2010, p. iii), in the US, Europe and beyond (de Vriend 2006; Balmer and Martin 2008), have similarly adopted the synthetic biology title, framing their research activities within the methodological and rhetorical scope of a science that strives to make biology 'engineerable' (Deplazes 2009). Dedicated synthetic biology programs have been established at universities; new sources of funding have been created; new firms and industries have adopted synthetic biology techniques; and the annual International Genetically Engineered Machine (iGEM) Competition[4] draws together student teams from around the world (de Vriend 2006; Balmer and Martin 2008). Add to this, a growing number of 'non-institutional' biologists (also known as 'DIY-biologists', 'amateur biologists', 'garage biologists' or 'biohackers') working outside of 'traditional' research settings (Schmidt 2008; NSABB 2010, 2011), and one finds that synthetic biology's disciplinary and institutional boundaries are decidedly blurred, while 'synthetic biology' (as an idealized vision for an emerging science) has gained momentum as a new way of thinking about modern biology. For example, although conducting very different types of projects than their institutional counterparts (having fewer technical and financial resources and working in informal research settings, including 'community labs'), amateur biologists have, in many ways,

[4] The iGEM competition is an annual event where "[s]tudent teams are given a kit of biological parts at the beginning of the summer from the Registry of Standard Biological Parts … and use these parts and new parts of their own design to build biological systems and operate them in living cells" (http://igem.org/About).

become emblematic of synthetic biology, if only because the trend towards non-institutional science suggests what might be possible "as more and more people have the necessary skills to engineer biology" (Schmidt 2008, p. 1).

Thus, within ten years, a small but growing 'synthetic biology community' is said to have emerged (de Vriend 2006; Tucker and Zilinskas 2006; Balmer and Martin 2008), composed of individuals with diverse technical backgrounds; occupying diverse (non-)institutional spaces. Yet, unambiguously defining a set of characteristics and practices that constitute 'synthetic biology proper', beyond the overarching aim of making biology 'engineerable' (Deplazes 2009), remains problematic.[5] What can be said is that synthetic biology is a distinctly interdisciplinary field, blurring the boundaries between biology and engineering, and between 'institutional' and 'non-institutional' science. Moreover, according to some (for example, de Vriend 2006; Schmidt 2008), it is precisely this blurring of boundaries that "distinguishes synthetic biology from genetic engineering and 'classical biology'" (de Vriend 2006, p. 63). At once characteristic of a science that promises to 'deskill' the 'craft' of genetic engineering (Mukunda et al. 2009) and suggestive of its potential, as "more and more individuals without a traditional education in biology or genetics (and probably even without higher education)" learn "to manufacture biological systems" (Schmidt 2008, p. 4), some believe "synthetic biology might finally unleash the full potential of biotechnology and spark a wave of innovation" (ibid, p. 1). From this perspective, synthetic biology is perceived to foreshadow the "domestication of biology", suggesting tantalizing opportunities, but also "unprecedented" risks (ibid.).

[5] A number of authors have attempted to further differentiate distinct projects or sub-disciplines within synthetic biology (see, for example, Benner and Sismour 2005; Balmer and Martin 2008; Deplazes 2009). Although offering further categories within which to group various research activities, all of which "can lay claim to the title 'synthetic biology'" (Benner and Sismour 2005, p. 542), the overarching theme is "the idea of turning biotechnology into a true engineering discipline" (Deplazes 2009, p. 428).

1.3 Risks and regulatory challenges

Although synthetic biology has, in recent years, attracted significant attention in light of its promising applications, it has simultaneously raised significant concerns about its potential risks and wider social and ethical implications. On the one hand, these concerns closely resemble those associated with earlier debates on 'recombinant DNA technology', including uncertainties about the unanticipated health effects and environmental consequences of 'genetically modified organisms'; ethical dilemmas associated with 'tinkering with nature' or 'playing god', and concerns about the commodification of life – patenting genes, genomes or organisms (ETC Group 2006; Balmer and Martin 2008; POST 2008). With a view to these concerns, synthetic biology is sometimes described as 'evolutionary' rather than 'revolutionary', essentially offering a different mode of arriving at the same 'kinds' of social and ethical implications. Indeed, it is sometimes suggested that much of what is presently called 'synthetic biology' is really just an extension of recombinant DNA technology, and therefore the science's 'implications', including its potential risks, are much the same. As the genetic engineers Benner and Sismour (2005, p. 541) argue, adopting a position often taken by advocates of synthetic biology against potentially more intrusive forms of oversight and regulation: "Placing a new name on an old technology does not create a new hazard."

On the other hand, just as many accounts suggest that synthetic biology offers "greater promise" and poses "greater perils" than any of the sciences or technologies from which it is derived (Samuel et al. 2009, p. 7). In particular, in light of advances in synthetic genomics and heightened concerns about '(bio)terrorism',[6] especially in the United States (Garfinkel et al. 2008; POST 2008; Lentzos 2009; Torgersen 2009), concerns have been raised about the potential *de novo* synthesis of

[6] 'Terrorism' and 'bioterrorism' ('terrorism' that deploys pathogens as weapons), as well as a variety of other terms that characterize the risk and security discourses discussed in my thesis, are contested (frequently highly politicized) concepts, which vary according to the social and political context within which they are deployed. In policy settings, 'terrorism' is broadly defined as a 'mode of political violence perpetrated by non-state actors against civilian populations', whereas 'terrorism', as a political label, is increasingly applied to just about "anything which involves destabilization of the normalized order of society" (Lipschutz and Turcotte 2005, p. 30).

dangerous pathogens that could be used to cause 'deliberate harm' (NSABB 2006; Garfinkel et al. 2007). With a view to these concerns, several high-profile experiments (for example, Cello et al. 2002; Tumpey et al. 2005) have received particular attention. In the case of 'synthetic poliovirus' (Cello et al. 2002), one of the earliest and most frequently cited examples of this type of experiment, Garfinkel et al. (2007, p. 6) suggest it, "demonstrated for the first time in a post-September 11 world the feasibility of synthesizing a complete microorganism – in this case, a human pathogen – using only published DNA sequence information and mail-ordered raw materials." For Garfinkel et al, and for others concerned about synthetic biology's potential 'biosecurity'[7] implications, experiments of this kind point to new 'risks' and 'regulatory challenges', as they suggest it is increasingly possible for individuals to synthesize microorganisms 'from scratch', including a list of high-risk pathogens presently under regulatory control (known, in the US context, as 'Select Agents')[8] (NSABB 2006; Garfinkel et al. 2007). More worrying still, from the perspective of these commentators, synthetic genomics could yield novel, taxonomically unclassified pathogens (thus absent from pre-existing control lists) more dangerous than those presently found in nature (ibid.).

Magnifying these concerns, the recent synthesis of a more virulent strain of avian influenza, intended to test the 'pandemic potential' of the H5N1 virus, sparked global controversy over the question of whether or not to publish the research protocols developed by two research teams (see, for an overview, Enserink and Malakoff 2012; Garrett 2012). Specifically, concerns were raised about individuals or terrorist groups repeating the published procedures, thereby gaining access to a

---

[7] Broadly, 'biosecurity', a concept that is relatively new to the life sciences, has been described by the World Health Organization (WHO) as consisting of measures aimed at "reducing the risk of unauthorized access, loss, theft, misuse, diversion or intentional release of [dangerous biological materials]" (WHO 2006, p. 11). In contrast, 'biosafety', which has a relatively long tradition in the life sciences, broadly refers to measures aimed at "reducing the risk of unintentional exposure to pathogens and toxins or their accidental release" (ibid). Although I will discuss both concepts in further detail in my thesis, for more detailed definitions at this time, see http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf.

[8] See http://www.selectagents.gov.

pathogen that could, "in the hands of malevolent individuals, organizations or governments", pose "an unimaginable catastrophe for which the world is currently inadequately prepared" (Berns et al. 2012, p. 153). Not only signaling the feasibility of creating pathogens more dangerous than those presently found in nature, reconfirming concerns about synthetic genomics and the limitations of 'list-based' approaches to regulation, these experiments brought to the fore an emerging set of policy concerns and regulatory dilemmas associated with access to 'dangerous knowledge', the communication of 'dual-use research', and what role (if any) censorship should play in the contemporary life sciences (Rappert 2003).

In the longer term, it is often said to be synthetic biology's capacity to 'deskill' bioengineering (a possibility often associated with the 'parts-based' approach to synthetic biology and concerns about an emerging 'hacker culture')[9] that the scope of synthetic biology's risks (as well as its possibilities for innovation) are viewed as infinitely expandable. As Mukunda et al. (2009) suggest, based on a series of interviews with "leading synthetic biologists" and "practicing biosecurity authorities" in the United States (ibid, p. 2), it is precisely "synthetic biology's focus on decreasing the skill necessary to modify biological systems and its emphasis on modular design" that new biosecurity risks and regulatory challenges are likely to emerge (ibid, p. 4). The expectation being, developments of this kind could eventually enable 'anyone' (including those who may wish to cause deliberate harm) to engage in potentially dangerous research. Although widely accepted that synthetic biology's 'deskilling agenda' (ibid.) has yet to be fully achieved (that is, genetic engineering remains more complex than the concept of a 'BioBrick' would suggest), 'if successful', the argument goes, there will be many more opportunities for the accidental or 'deliberate misuse' of modern biology (NSABB 2006, 2010; Mukunda et al. 2009; Purnick and Weiss 2009; Kwok 2010; NRC 2011).

In this context, it is apparent that the promise of synthetic biology to enable the construction of (novel) biological entities and to 'democratize' bioengineering,

[9] See Schmidt (2008, p. 2), who describes "a new kind of hacker culture, the 'biohacker'", which "means designing and manufacturing biological systems in an open way but hardly any kind [*sic*] of regulatory oversight or enforcement in place."

possibilities that have garnered great interest from governments, technologists and industries in recent years (Carlson 2008), have simultaneously made the science the focus of an opposing set of expectations. A so-called 'dual-use biotechnology' (NRC 2004), synthetic biology is believed to be capable of enabling tremendous benefits and tremendous risks – new avenues for 'bioeconomy' and 'bioterrorism' (NRC 2011). In this light, the 'success' of synthetic biology, and, with it, the promise of new forms of 'health' and 'wealth', is believed to depend upon fostering the former while preventing the latter. Yet, "[h]ow can possible risks associated with the generation of novel organisms be addressed" (NSABB 2006, p. 15)? How can regulations be devised to avoid "unnecessarily hampering the pace of research while managing risk" (ibid, p. 9)? How can "regulators … devise a legislative and regulatory system that balances security and safety risks to facilitate research without imposing unreasonable bureaucratic burdens on scientists and academic freedom" (Samuel et al. 2009, p. 8)? What sorts of 'options for governance' are needed to ensure that synthetic genomics achieves its full potential (Garfinkel et al. 2007)? These are among the many practical considerations and instrumental goals that characterize an ongoing regulatory process that seeks to 'secure' and 'sustain' a science characterized by sharply contrasting expectations.

1.4 Regulatory governance

In light of synthetic biology's 'dual-use potential', it is widely believed (including among some synthetic biologists) that some form of 'regulation' is needed to ensure the science can proceed 'responsibly'. In the United States, in particular, these concerns have, in recent years, motivated regulatory authorities to seek scientific and technical guidance on how to 'assess' and 'manage' synthetic biology's 'biosecurity risks' (see, for example, NSABB 2006, 2010; DHHS 2010b; PCSBI 2010). Justified not only on the basis of mitigating potential harm, but also on the basis of fostering innovation and industry, the overall aim of these initiatives has been to identify "relevant policy actions targeted to promote risk management, while seeking to minimize negative impacts upon scientific progress or industrial

development" (DHHS 2010b, p. 2). With a view to this objective, synthetic biology and synthetic biologists (as the innovators and practitioners most directly engaged in the development and application of the science) have emerged as the focus of an assortment of risk assessment activities and risk management strategies explicitly (if not self-consciously) aimed at balancing potentially competing demands for 'scientific freedom' and 'national security'.[10] What is more, it has been with a view to 'risk' and its 'management' that this outcome is perceived to be possible.

This framing of synthetic biology – as a 'risk' to be 'managed' – is indicative of a growing trend towards the (re)characterization of regulatory subject matter in terms of 'risk', and underpins the concept of 'risk regulation' (Fisher 2010). As Bridget Hutter (2005) suggests, 'risk-based' regulation is intended "to help governments, regulatory agencies and companies manage risks more effectively and prioritize actions and resources accordingly" (ibid, p. 13). Traditionally, risk-based approaches to regulation have aspired to 'objectively' measure risk, promoting "the use of technical *risk-based tools*, emerging out of economics (cost benefit approaches) and science (risk assessment techniques)", suggesting a level of formal calculation (ibid, p. 3, emphasis in original). The benefit of such approaches is often said to rest in their capacity to "constrain discretion" and to enhance the objectivity of policy decisions (Fisher 2010, p. 51). Moreover, from the perspective of regulators, they are said to offer a more or less explicit accounting of their risk assessment and risk management activities, enabling greater transparency, and ultimately a justification for their regulatory decisions in the face of potential criticism for doing too little or too much to regulate (Majone 2010).

Historically, this approach to regulation has been applied to a limited sphere of regulatory activity (notably, health and environmental risks), but in more recent years risk-based approaches have come to be applied to a much broader range of issues, ranging from financial crisis to terrorism. At the same time, risk-based

[10] McLeish and Nightingale (2007, pp. 1636-1637) underline that this "dilemma" is characteristic of wider regulatory discussions directed at modern biology, namely: "how to design policies that can simultaneously successfully suppress biological weapons development whilst accommodating and even encouraging the spread of dual use technologies for legitimate technical and scientific reasons?"

techniques have expanded from the use of highly technical, probabilistic methods of assessment ('quantitative risk assessment') to a broader array of techniques, ranging from scenario analysis to expert judgment. Even though these techniques may have little to do with 'quantifying' risk, they are nonetheless intended to enable 'reasoned estimation' (O'Malley 2004) and to lend a sense of 'process' to regulatory decision-making (Power 2004). Today, adherence to 'risk regulation' may range from the simple use of 'risk regulatory concepts' (Fisher 2010), such as 'risk', 'risk assessment' and 'risk management', to the use of 'traditional' "risk-based tools derived from economics and science" (Hutter 2005, p. 6). Moreover, adherence to such approaches may be *ad hoc* or an integral component of an overarching regulatory strategy (ibid.). Irrespective of their adherence to quantitative methods, risk-based approaches have become synonymous with discourses on 'good governance' (Power 2004) and are increasingly central to notions of 'better regulation', serving, in many ways, as "a badge of legitimacy" (Black 2010, p. 89).

In this light, it is perhaps not surprising that the notion of 'risk' is an integral feature of how the 'deliberate misuse' of synthetic biology is currently represented in regulatory contexts, and that 'risk assessment' and 'risk management' are promoted as favored regulatory instruments. To what extent this characterization of synthetic biology represents a highly technical mode of assessment, or whether concepts such as 'risk', 'risk assessment' and 'risk management' play a more rhetorical function, is uncertain. At the very least, the deployment of this language is intended to suggest a more or less structured regulatory process, one that may "offer a principled way of organizing what we know about the world" (Jasanoff 1993, p. 129). Moreover, whether by rigorous quantification or qualitative interpretation, this characterization of 'deliberate misuse' reinforces the expectation that synthetic biology's 'risks' can be made the subject of 'regulation' or 'risk management', a distinction that is increasingly blurred (Power 2007). In this context, what is of particular analytical interest is "the overall approach to regulating", a concept known as "'regulatory governance'" (Wiener 2010, p. 140), adopted to enable synthetic biology to be 'governed through risk'.

1.5 Outline of my argument

It has been suggested that, following the events of 9/11, and the subsequent anthrax letter mailings, "[t]he dread of nuclear, biological and/or chemical terrorist attacks moved to the forefront of arguments about the inability to estimate the severity of loss" (Erickson and Doyle 2004, p. 214). For some risk scholars, these events reconfirmed their belief that we are living in a 'post-risk-calculation' world (Beck 2002), one populated by self-generated risks for which we do not have, and cannot have, 'the knowledge or the measure'.[11] Yet, others disagree, and not simply on the basis of their own risk theories, but on the basis of the diverse 'risk-based' techniques that are continually being developed, adapted and deployed to assess, manage, and insure against all sorts of modern hazards, including 'catastrophic' acts of 'terrorism' (Erickson and Doyle 2004; Lakoff 2006; Lakoff and Collier 2008). Although these techniques do not necessarily depend upon the use of statistical methods, traditionally favored as an 'objective' mode of risk assessment, they nonetheless represent legitimate attempts at 'ordering uncertainty' in such a way that it might be 'governed'. Thus, from the perspective of these risk scholars, it is worthwhile to attend to these new sites of risk assessment and risk management, as they suggest new ways of understanding and intervening upon a diverse range of social problems. In brief, it is fruitful to consider how, *in practice*, issues such as terrorism, climate change and financial crisis are viewed as destabilizing previous ways of understanding the world, yet are governed in a variety of ways, beyond the limits of "meaningful statistics" (Erickson and Doyle 2004, p. 18).

The ongoing regulatory effort in the United States directed at synthetic biology – an emerging science that promises to 'democratize' bioengineering – and its potential misuse in an act of 'bioterrorism' represents one site of risk assessment and risk management that does indeed contradict Ulrich Beck's (1992) grand claim that we are living in a 'post-risk-calculation' or 'post-insurance' age. This is because a variety of risk-based techniques and regulatory strategies are presently being

[11] Adapted from François Ewald's (2002, p. 294) description of "a risk beyond risk, of which we do not have, nor [*sic*] cannot have, the knowledge or the measure."

developed, adapted and deployed to govern this highly specific – by some accounts, 'potentially catastrophic' – problem. Not only do these efforts demonstrate that such risks can be made the subject of highly specific forms of regulatory intervention and control, but, moreover, that there is (within government agencies, federal bureaus, *ad hoc* committees, working groups, scientific academies, biotech companies, think tanks and laboratories, based in the US and elsewhere) a distinct will to do so. If 'governing through risk' in the context of synthetic biology – in the context of 'catastrophic terrorism' – can tell us anything about the 'limits' of 'risk calculation', it is that these limits are restricted only by the imagination.

My thesis, in turn, engages with a 'risk management process' that is, in a highly instrumental sense, enabling synthetic biology (as a science, an industry, and a source of seemingly boundless expectations) to move forward. It attends to a specific kind of social problem – one that exists at the interface of 'biotechnology' and 'national security' – and the "constellation of experts" (Rabinow 2008, p. 279), ranging from public health officials to law enforcement agents and biodefense scientists, who have assembled around this problem to develop *practical* solutions. I emphasize this term because 'pragmatism' filters through all aspects of the ongoing regulatory response that has been mounted against the deliberate misuse of synthetic biology. Most of all, it is visible in the discursive and non-discursive practices of scientific and technical experts who have been called upon to anticipate and (to the extent possible) prevent risks of this kind, and who believe that this objective is not only possible, but also that it is possible (with the right 'mix' of risk assessment techniques and regulatory strategies) to simultaneously ensure that the science fulfills its anticipated potential. In other words, for these scientific and technical experts, it is *possible*, even in the face of 'potential catastrophe', to both 'secure' and 'sustain' synthetic biology through risk management.

Of course, this theme is not all together new. Previous biotechnologies – most notably, recombinant DNA technology in the 1970s – have been framed as both (potentially) 'catastrophic' and (ultimately) 'manageable'. Regulatory controls were developed in the belief that intractable uncertainties need not prohibit scientific progress. Yet, the case of synthetic biology is not simply a repetition of what has

come before, and not only because the science is perceived to be endowed with unique attributes – offering the possibility of unparalleled risks (Samuel et al. 2009, 'Managing the unimaginable: Regulatory responses to the challenges posed by synthetic biology and synthetic genomics') – but also because it is embedded in a specific historical moment, one that favors a different view of 'risk' in the life sciences. Namely, synthetic biology is the first iteration of biotechnology to be framed first and foremost as a '(bio)terrorist threat', a type of 'deliberate catastrophe' that suggests a "pervasive sense of disestablishment" that "strikes at the cultural foundation of risk society" (Erickson and Doyle 2004, p. 14). Today, in contrast to earlier debates on recombinant DNA technology, it is primarily with a view to 'deliberate misuse' (Rappert 2003; Reppy 2003; McLeish and Nightingale 2007; Collier and Lakoff 2008), rather than 'unintended consequences', that synthetic biology's 'risks' are understood, represented and made the subject of regulatory intervention and control. Indeed, synthetic biology represents an exemplar of 'dual-use biotechnology' in an 'age of terrorism' (NRC 2004), serving as both an example of how modern technological risks are assessed and managed, and as a vector through which to explore how the contemporary life sciences are being reconfigured through their pairing with concerns about bioterrorism.

In the vein of research projects interested in regulatory design and administration, ranging from studies on financial crisis to terrorism, my thesis seeks to engage with how notions of 'risk' are brought to bear on a complex hazard and ultimately "how regulatory authorities put into operation risk-based approaches to achieve their regulatory goals" (Bounds 2010, p. 27). My thesis, in turn, examines the discursive and non-discursive practices presently enacted by scientific and technical experts engaged in 'selecting', 'assessing' and 'managing' the diverse risk aspects of synthetic biology in pursuit of a 'secure' and 'sustainable' science. With a view to this overarching research aim, my primary research questions ask: How is synthetic biology understood and represented as a 'biosecurity problem'? How is this problem rendered 'knowable' and 'calculable' through risk assessment techniques? What risk management strategies are proposed to mitigate these risks, and how are these justified? And, finally, what forms of 'risk responsibility' do these

strategies seek to engender in synthetic biologists, and to what effect? These questions are intended to shed light, not only on the techniques whereby problematic people and things are made the subjects of risk management or regulation, but also on the normative and performative dimensions of 'governing through risk'. In this manner, this research seeks to open up space for critical reflection on the kinds of risks synthetic biology and synthetic biologists are taken to be, how these risks are assessed and managed through risk-based techniques, and the kinds of responsibility for managing risk these seek to engender in those engaged in various aspects of the science and its management.

1.6 Structure of my thesis and summary of chapters

My thesis attends to a 'risk management process', which, for the scientific and technical experts consulted for my research, represents a 'scientific' or 'technical' approach to 'risk management' or 'regulation', consisting of several distinct 'steps', typically defined as: 'risk identification', 'risk assessment' and 'risk management'. For these experts, this process represents a linear, scientific procedure (Fisher 2010) and marks the boundaries of 'objective risk assessment' and 'rational policy-making'. However, while this thesis attends to this process, it does so with a very different perspective on its presupposed linearity, procedural clarity, and scientific rationality. In practice, and in stark contrast to this idealized vision of science policymaking, my thesis underlines that there is no singular or best way to 'govern through risk', and the risk management process in synthetic biology is guided and constrained less by the availability of scientific knowledge and systematic standards of measurement, and more by the very capacity of governmental actors and organizations to design and produce risk management procedures, protocols and guidelines that are used to inform and to justify risk management actions that seek to enable a 'secure' and 'sustainable' science. In the following chapter summaries, I will provide a brief overview of the argument developed in my thesis, highlighting how, and to what effect, synthetic biology is 'governed through risk'.

In Chapter 2, I situate my research in the risk literature in sociology, identifying two broad schools of thought on risk, as a 'calculative rationality', and the perceived limits of 'risk calculation'. On the one hand, I introduce Ulrich Beck's (1992) 'risk society' thesis, which argues that there exist today technological hazards that exceed the very limits of risk and insurance, suggesting the emergence of a 'risk beyond risk', one that cannot be rationally assessed. Risk society theorists call into question not only the epistemological limits of risk to calculate potential loss – where 'risk' is defined as a probabilistic measure based on 'quantitative risk assessment' – but also cast doubt on the authority of risk experts who claim that immeasurable dangers can be assessed and managed. On the other hand, and in contrast to this more or less 'realist' perspective on risk, I introduce the work of theorists who have drawn on Foucault's concept of 'governmentality' to develop an alternative interpretation of risk, as a 'governmental rationality'. For these theorists, risk is not an objective fact that can only be calculated on the basis of statistical measurement, but rather it is a category of understanding, a way of ordering reality in such a way that it might be governed. It is with a view to the latter body of theory, I argue, that one is able to account for diverse sites of risk assessment and risk management that characterize various 'risk regulation regimes' or 'regimes of government', including the case of synthetic biology examined in my thesis, which may not rely on numbers and statistics to validate knowledge claims about an uncertain future, but are no less concerned with organizing uncertainty, enabling action in the present. In this light, risk is not limited by the availability of scientific knowledge, but rather it is infinitely adaptable and takes on multiple and heterogeneous configurations.

Chapter 3 outlines my research methods, offering a rationale for my research design and outlining the research process undertaken to answer my research questions. In the first instance, I argue that an 'analytics of government' provides a suitable analytical framework for my thesis, as well as a basis for my research design, in as much as this approach to risk pursues a consistent line of questioning geared towards understanding how 'regimes of government' or 'regimes of practices' operate (Dean 1999). In the second instance, I describe the research process,

including my identification of the social group (a 'constellation of experts' engaged in 'biosecurity policy') of primary interest to my thesis and the 'qualitative research methods' (including document analysis, expert interviews and observations in the field) selected to shed light on the discursive and non-discursive practices that comprise the 'risk management process' examined in my thesis. Finally, I consider my own role in the research process, reflecting on how my choices have played an integral role in determining the 'scope' and 'quality' of my research. Taken together, this chapter describes a qualitative research project designed to understand *how* scientific and technical experts render a seemingly 'incalculable risk' 'knowable' and 'actionable' in pursuit of a 'secure' and 'sustainable' science.

With a view to risk management or regulation as a 'process', Chapter 4 examines what is very often overlooked by various scientific and technical experts engaged in assessing and managing 'new' and 'emerging' risks in the life sciences – namely, these 'risks' are neither innate nor inevitable. Rather, they are contextually situated and defined through a demanding process of selection and classification. In the case of synthetic biology, what is perceived to be problematic about the science can be traced to growing concerns about 'bioterrorism' and heightened demands for 'biosecurity' – a defensive practice premised upon keeping 'dangerous tools' out of 'dangerous hands' (the 'classical' biosecurity model). Drawing on the biosecurity policy literature and interviews with synthetic biologists and experts specializing in aspects of biosecurity, this chapter introduces how synthetic biology – a science that promises to 'democratize' modern biology – is perceived to be fundamentally at odds with biosecurity practices premised upon a logic of 'command and control'. Synthetic biology, I suggest, is undergoing a process of 'problematization', as it has destabilized previous ways of understanding the world, motivating a regulatory response that seeks to reestablish order in the face of uncertainty and change. It is with a view to 'risk selection', the subject of this chapter, whereby new risks are identified, classified and given a name, that problematic people and things are made subjects and objects of regulatory attention and political deliberation.

Chapter 5 moves beyond risk as a category or label signifying potential harm towards risk as a mode of measurement or calculation. Risk assessment in the context of science policymaking, introduced at the beginning of this chapter, although aspiring to the regulatory ideal of 'quantitative risk assessment', does not follow a preexisting standard, much less a 'scientific' one. In fact, risk assessments, especially in the case of emerging technologies, which are characterized by scientific unknowns and numerous 'potential benefits' as well as 'potential risks', are not only intended to be reasonably 'precise' – representative of the 'actual' risks – but also 'practical' – enabling regulatory interventions that satisfy a variety of policy objectives, including aspirations for regulatory consistency and scientific and economic development. In the second part of this chapter, I argue that this 'pragmatic' approach to policymaking is indicative of regulating biotechnology, both the present case of synthetic biology and the earlier case of genetic engineering (a precursor to synthetic biology). In both instances, regulatory strategies have been designed to make 'novel' risks 'fit' (through a combination of risk assessment techniques, both quantitative and qualitative) existing regulatory frameworks and specific risk management objectives. Finally, this chapter concludes with a detailed case study on 'biosecurity risk assessment' in the context of the DNA synthesis industry, a site of intense regulatory interest and concern. An instance of 'pragmatic policymaking', recent federal guidelines developed for DNA synthesis providers describe a more or less structured risk assessment procedure or process (drawing on an assortment of 'risk-based' techniques and regulatory strategies) used to inform and to justify risk management decisions, enabling DNA synthesis companies to process orders in the face of seemingly intractable uncertainty.

This 'pragmatic' approach to science policymaking extends to all aspects of the ongoing regulatory process in synthetic biology, which not only seeks to 'secure', but also 'sustain' an emerging science. Chapter 6 considers how this desired balance is brought into conflict with a host of policy proposals and regulatory strategies that ascribe to the 'classical' biosecurity model, which depends upon restricting access to science. The first part of this chapter considers two broad families of proposals of

this kind, one directed at controlling access to tangible biotechnologies and the other intangible life science knowledge. Significantly, although both sets of proposals share a common preoccupation with questions of access to science, growing concerns about 'dangerous knowledge' (as opposed to dangerous pathogens, laboratory equipment or other tangible artifacts) suggest an increasingly precautionary approach to biosecurity, raising concerns about constraints on scientific freedom, which some fear may diminish scientific progress. The second part of this chapter then considers how recent concerns about the publication of H5N1 ('bird flu') research has motivated new federal policy on 'dual-use research of concern', which combines aspects of earlier proposals under a singular risk management standard, one that attempts to negotiate the scientific uncertainties and administrative challenges associated with anticipating and preventing the production and distribution of 'forbidden knowledge'. The final part of this chapter then sheds light on an alternative biosecurity model, one that has largely been advanced by social scientists and is gaining growing support among biological weapons experts, which calls into question the effectiveness and desirability of preventing access to science, suggesting the need for a new approach to biosecurity, one that attempts to shape the conduct of scientists themselves.

Chapter 7 examines what is increasingly perceived to be among the most sustainable 'solutions' to the seemingly intractable policy 'problem' of synthetic biology, namely, 'self-governance'. The first part of this chapter underlines how recent calls for a new 'culture of responsibility' have begun to place new demands on scientists, who are increasingly encouraged to play an active role in biosecurity. With a view to 'biosecurity', in contrast to 'biosafety', scientists are desired to be both prudent ('self-disciplined') and vigilant ('watchful'), enabling them to take on much of the day-to-day responsibility of 'policing science', while simultaneously bringing the worlds of 'science' and 'national security' into closer contact. The second part of this chapter then looks in-depth at a variety of biosecurity awareness raising activities, in particular the FBI's ongoing engagement with (amateur) synthetic biologists, which aim to provide scientists with the situational awareness

to anticipate potential biosecurity risks within their 'communities'. Although, for many, including many synthetic biologists, 'self-governance' is perceived to be desirable, as it might limit regulatory constraints on science, there remain doubts about the effectiveness of the 'self-governance' biosecurity model and ambivalent attitudes on the part of scientists about the desirability of 'policing themselves'.

Finally, in Chapter 8, I reflect on several key themes that have emerged from my research, and which have been examined in my thesis, drawing attention to, on the one hand, risk's capacity as an adaptive 'technique of government' and, on the other, its capacity to not only describe, but also produce the very 'risks' it seeks to visualize and control. In relation to the first theme, my thesis underlines that there are, quite literally, 'no risks beyond risk', as 'risk' and 'risk thinking' are defined and constrained, not by the availability of scientific knowledge (exemplified by numbers and statistics), but by the very capacity of governmental actors and organizations to (re)imagine and (re)configure 'uncertain futures' as 'calculable risks'. Contributing to recent risk scholarship in sociology, which has endeavored to examine how 'risk-based' techniques are brought to bear on all sorts of modern hazards, my thesis demonstrates that, in the absence of numbers, much of the 'work' of risk management in the context of regulating synthetic biology leverages on experts' determination to design and construct rationalized processes, protocols and procedures that are intended to achieve 'practical' policy 'solutions' to complex policy 'problems'. In relation to the second theme, my thesis sheds light on the normative and performative dimensions of 'governing through risk', which, in the case of synthetic biology, is shifting attention to concerns about bioterrorism, and influencing the manner in which scientists, security professionals, regulators (indeed, all of us) understand and represent modern biology.

2. Theory and the 'how's' of risk-based government

2.1 Introduction

Whether the potential misuse of synthetic biology constitutes a 'calculable risk' or 'incalculable danger' is uncertain. At best, such a distinction would be an arbitrary one, as the future cannot be known with certainty. Although acknowledging that self-generated risks produced by advanced, industrialized societies (Beck 1992) challenge a risk calculus that calls for stable facts – expressed since at least the early nineteenth century in terms of probabilities (Hacking 1990) – about the activities of people and the capacities of things, this research seeks to avoid grand claims about what kind of risk (or danger) synthetic biology might 'actually' pose. It also seeks to avoid making prescriptions for the 'proper' way of governing in the face of uncertainty. Instead, it focuses on the discursive and non-discursive practices presently enacted by diverse experts in the name of selecting, assessing and managing the unruly aspects of synthetic biology in pursuit of a 'secure' and 'sustainable' science. Whether potential events are imagined as risks or as dangers, such practices share the common goal of negotiating and (more or less successfully) ordering uncertainty, enabling action and intervention in the present.

At its foundation, then, this research is concerned with a type of governmentality,[12] where risk can be understood as "a way of representing events in a certain form so they might be made governable in particular ways, with particular techniques and for particular goals" (Dean 1999, p. 177). In this context, risk is neither viewed as a monolithic technology nor as one driven by inescapable

[12] See Burchell, Gordon and Miller (1991) for their edited volume on Michel Foucault's concept of governmentality. See, also, Mitchell Dean's (1999) book on *Governmentality: Power and rule in modern society*. Based on my reading of Foucault, and guided by my reading of the theorists discussed in this chapter, I take 'governmentality' to mean 'mentalities of government' or the 'art of government', which, I argue, is an interpretation that fits well with the notion of 'governing through risk' in the context of synthetic biology, as it suggests that risk is an adaptive 'technique of government' applied to the selection, assessment and management of diverse social problems.

forces of modernization, but rather as "a complex category made of many ways of governing problems" (O'Malley 2004, p. 7). With a view to this conceptualization of risk, my thesis contributes to a growing body of risk scholarship (for example, Erickson and Doyle 2004; O'Malley 2004; Bigo 2006; Aradau and van Munster 2007; Lakoff and Collier 2008) concerned with how risk and security professionals (Bigo 2000, 2006) select, assess and (at least ostensibly) manage potential 'catastrophes', ranging from climate change to terrorism, that would seem to challenge, if not undermine, a scientific rationality that claims to be based on objective knowledge about the world. As opposed to collapsing the prudential enterprise of risk, inviting an era of 'post-risk-calculation' and limitless 'precaution', this literature suggests that efforts to lay claim to an uncertain future are proving to be more responsive and adaptive than 'risk society' theorists would contend. In particular, in the face of extreme uncertainty, non-quantitative modes of risk-based government, which increasingly draw on the subjective expectations and professional judgments of diverse experts as the source of their authority, are increasingly being taken up and deployed side-by-side more 'classical', quantitative risk-based techniques.

In this chapter, I will, first, introduce some of the key theory that will be drawn on throughout my thesis, illustrating how risk, taking on multiple and heterogeneous configurations, can be conceived as a 'mode of government'. I divide this theory into three sections – (1) making up problems, (2) problems of measurement and (3) anticipatory government – in an effort to organize the conceptual framework for my thesis. Although broadly mirroring the successive 'steps' – risk identification, risk assessment and risk management – scientific and technical experts use to characterize the risk management or regulatory process, this chapter presents a very different view of the presupposed 'linearity' and 'scientific rationality' of this 'process'. Specifically, the 'risk management process' explored here, and throughout my thesis, is one characterized as much by experts' attempts at 'organizing uncertainty' through forms of classification and structured reasoning (and other 'qualitative' forms of measurement) as it does highly technical modes of 'risk calculation'. Second, I will situate this theory more concretely in the context of 'regulatory governance', where 'governance' refers to "the overall mode

or approach of governing" (Wiener 2010, p. 140). Third, I will conclude this chapter by way of introducing how an 'analytics of government' – concerned with the 'how's' of governing, attending to the specific and not the general; informing a consistent line of questioning that is geared towards understanding how 'regimes of practices' of government operate (Dean 1999) – not only informs risk theory, but also serves as an analytical framework for the study of risk, helping guide where one looks for data, as well as the kinds of questions one seeks to ask of that data.

2.2 Making up problems

In the tradition of social and cultural studies on risk (Bradbury 1989), my thesis starts from the premise that 'risk' – and the various 'social problems' (Schneider 1985) defined in its name – is not an intrinsic attribute of objects that exists beyond the social world. Rather, risk can more appropriately be thought of as, "a kind of conceptual umbrella used to cover all sorts of events, be they individual or collective, minor or catastrophic" (Ewald 2000, p. 366). To speak of risk in this way, is to underline that risk is (at least in part) 'socially constructed' (Berger and Luckmann 1966) – "the outcome of a process of collective definition" (Blumer 1971, p. 298) – and not an objective 'fact' about the world as it 'actually' is. In the context of my thesis, the strength of this conceptualization of risk rests in its capacity to shift the locus of analytical attention from the various technological artifacts and possible future harms associated with synthetic biology towards the discursive and non-discursive practices enacted by scientific and technical experts engaged in selecting and naming new 'risk objects' – things, activities or situations "deemed to be sources of danger" (Hilgartner 1992, p. 40) – for regulatory attention. In this light, the primary 'object' of interest in my thesis is not so much the 'first-order' (Luhmann 1993) problem of synthetic biology-enabled 'bioterrorism', but rather the various ways in which this problem is constituted by scientific and technical experts seeking policy solutions to an emerging set of concerns and dilemmas.

At the same time, this conceptualization of risk does not demand ignoring that events such as terrorism (when they occur) can and do have an objective

reality. Rather, it is to respect that this 'reality' is contingent and context bound. As Shelia Jasanoff (1993, p. 127) suggests: "What we claim to know about risk, how we acquire more information, and how we interpret the facts in our possession are all contingent on contextual factors, ranging from individual or organizational experience to national political culture." This perspective, in turn, places the investigation of risk squarely within the social world, permitting an analysis that favors a close reading of the social and political milieu within which risk discourses are embedded. For example, as Jasanoff (1990) has demonstrated in her work on science advisory committees in the United States, how risks are represented in regulatory processes varies according to institutional and national context (see, also, Hood et al. 2001), as well as the individual preferences of those considered competent to speak the 'truth' on ostensibly 'technical' questions about risk. By treating risk as a "socially constructed attribute", and not "as a physical entity that exists independently of the humans who assess and experience its effect", it is possible to make clear that "processes of risk identification … can never be value free" (Bradbury 1989, p. 381). Thus, while scientific and technical experts engaged in science policymaking tend to expend considerable effort attempting to differentiate between 'politics' and 'science', and between 'speculative' (non-scientific) and 'objective' (scientific) risk (an activity known as 'boundary work'), boundaries of this kind are inevitably blurred (Jasanoff 1990).

While a broader literature exists on the 'social construction' of 'social problems' (see, for example, Berger and Luckmann 1966; Blumer 1971; Kitsuse and Spector 1973; Rains 1975; Aronson 1982; Schneider 1985), which represents the origins (an observation made by Hacking 1999) of much of the theory introduced in this section, the following discussion is narrower in scope. Rather than seeking to establish a set of social processes that describe the "career and fate of social problems" (Blumer 1971, p. 301), the following theory is intended to help conceptualize the notion of risk as a 'social construct' and 'risk identification' as a social process. In particular, several themes are introduced that are of particular relevance to my thesis: First, the identification of new risks can primarily be understood as a 'social' rather than 'technical' activity. Second, claims about risk are

(in many ways) 'constitutive' of reality (Rains 1975), where the very act of naming new risks opens up new space for thought and action. Third, notions of risk abound in everyday life, and not simply because "threats are hovering over us", but because "[t]he perception of risk constitutes a defining experience for contemporary society" (Ewald 2000, p. 379). From the perspective of governmentality theorists, a perspective that informs my own theoretical stance, risks are "neither real nor unreal. Rather they are ways in which the real is imagined to be by specific regimes of government, in order that it may be governed" (O'Malley 2004, p. 15).

2.2.1 Securitization

Securitization theory (Wæver 1995), although an international relations concept and not a sociological one, provides a number of useful insights into the social processes involved in marking out new 'risks' (or, in this case, 'security threats') for critical attention. Unlike traditional approaches to security studies that assume that the perception of new threats are the natural consequence of rational assessments made by knowledgeable analysts (Lipschutz 1995), this theory proposes that security problems are the consequence of their naming as *matters of security* (Wæver 1995). In this context, the authoritative 'speech acts' (Austin 1955) of high-ranking government officials are said to mobilize security expectations, where the enunciation of the word 'security' signals a danger and sets a priority (Wæver 1995). Moreover, the word 'security', which is bound up with notions of 'national security', is said to organize expectations in a specific manner, namely around the themes of 'threat-vulnerability-response'. And, while this might be a fine way to frame certain threats, such as war and terrorism, Wæver and colleagues (Lipschutz 1995) argue that it may be an inappropriate framework for dealing with certain 'state-endorsed' security matters, such as 'environmental security' or 'health security'. This suggests that the 'security' label (like the 'risk' label) is both performative and problematic. Performative, in that, "[t]he naming is at once the setting of a boundary, and also the repeated inculcation of a norm" (Butler 1993, p.

8). And problematic, in that some problems (if one can speak of them as 'problems' in the first place) are not necessarily matters of *national security*.

Although a distinct departure from the dominant, realist view on security that conceives of threats as the material consequences of dangerous people and their technological capabilities (Lipschutz 1995), securitization theory remains of only limited value in the context of sociology. There are several reasons for this. First, despite efforts to distance itself from 'classical' security studies, securitization theory remains grounded in a state-level, hegemonic view of politics, which privileges the agency of political elites, while overlooking the words and actions of other, less prominent, but equally instrumental, actors (Bigo 2000, 2006; CASE Collective 2006; McDonald 2008). Notably, securitization theory has been criticized for failing to acknowledge the roles and daily routines of the many diverse bureaucrats and 'security professionals' (Bigo 2000, 2006), ranging from police forces to customs officials, who equally have a stated interest, and a perceived expertise, in a range of problematic issues that might be taken up and advanced as 'matters of security'. More generally, it has been suggested that securitization is "something that increasingly permeates everyday life in the form of risk management" (van Munster 2005, p. 10), and thus it is far more routine – less 'exceptional' – than securitization theorists contend (ibid.). Significantly, Didier Bigo (2000, p. 347) suggests, this more generalized perspective on securitization makes apparent that there is no "conspiracy" behind the security label – no single group or authority that "possesses a monopoly on this symbolic power." Rather, Bigo argues, "it is a field effect", not the outcome of a "one actor-narrative" (ibid.).

Second, securitization theory maintains an ambivalent relationship with state-level authority. On the one hand, it acknowledges the legitimacy of such authority, in as much as security continues to be framed, first and foremost, as a matter of 'national security', calling for state-level deliberation and, if necessary, state-level intervention. On the other hand, it suggests that powerful interests at the highest levels of government play a more or less active role in producing new security problems to protect the sovereignty of security institutions and the

monetary rewards stemming from security practice.[13] Although such intent might exist, it is speculative, and risks eliding the fact that mobilizing security expectations need not be driven by the self-motivation of government authorities (or any single actor or group for that matter), but could equally be (to name just one alternative) a matter of more or less informed intelligence about a particular threat, which could legitimately be in the interests of society to address and prepare for.

Finally, taken to the extreme, securitization theory risks becoming a totalizing, constructivist approach to security, concealing the materiality of the threats in question. Unavoidably, events, such as war or terrorist attacks (when they occur), have an undeniable impact on human life, which underlines that such events are more than just 'speech acts' and have significance beyond political rhetoric. Nonetheless, and largely due to its strict constructivist program, securitization theory serves as a reminder that threats do not exist 'out there', somewhere beyond the social world, but are entangled within it. Even if such an observation is familiar to sociologists, securitization theory, I would suggest, nonetheless has utility if only as a means of illuminating that security problems are 'problems' of a particular kind, which are quite familiar to international relations scholars, and perhaps less so to sociologists. Namely, security problems are often associated with 'states' and 'sub-state actors'; 'war' and 'terrorism', and are bound up with specific ways of thinking and talking about problematic people and things, which necessarily plays a significant role in shaping security discourses, as well as the security practices enacted in the name of security. Therefore, a limited engagement with securitization theory, and the language of security (often framed in terms of 'threat-vulnerability-response', as noted above) it is bound up with, can help add nuance to a critical, sociological analysis of how security problems come into being.

[13] Wæver (1995, p. 62) argues, for example, that, in the wake of the Cold War, the "security establishment" embraced the expansion of security to domains such as the environment in an effort to maintain "their own societal relevance, as well as providing jobs to 'security studies' and 'strategic studies' analysts."

2.2.2 Dynamic nominalism

Another, more modest, but altogether more grounded, approach to the analysis of how new problems and risks come into being is one that Ian Hacking (1990, 2002) develops through his historical research on risk, and the concurrent rise of statistics and probability. In particular, Hacking's concept of 'making up people' – a variety of 'dynamic nominalism' that conceives of risk as a mode of classification – describes a mechanism whereby risks are regularly produced and made the subject of social and political attention. Neither depending on authoritative speech acts nor on the involvement self-interested elites, Hacking's work represents a departure from securitization theory. Specifically, it underlines that risks can (and, indeed, are) produced through social processes that are by no means 'exceptional', but rather integral to contemporary life. Since the rise of statistics, Hacking argues, new kinds of people and things – new kinds of 'problems' and 'risks' – have been brought into being hand-in-hand with their naming and classification.

For Hacking, such labeling and classification can be traced to at least 1820, at a time when statistics, and the 'avalanche of numbers' that accompanied statistics, came to be systematically applied to all manner of 'deviant' community, including the mentally ill, criminals, prostitutes, and many others. At this time, Hacking argues, populations came to be understood in terms of the distributions of people that constituted them, which, in turn, showed predictable regularity, demarcating particular types of people that could subsequently be observed, assessed, and managed. Concurrently, Wilkinson (2010, p. 19) adds, "the framing of social problems as 'risks for society'" and "the identification of particular groups and individuals as 'risks to society'" contributed to "the emergence of social institutions, legal frameworks and expertise designed to protect and promote the nation's health, wealth and social well-being." In time, these categories of people were (and, in some instances, continue to be) taken-for-granted, as one could hardly dispute their existence once they were accounted for year after year in census data, much less after they had been made the subjects of specialist institutions, laws and

professions. In brief, once new categories of people came into being, they could no longer be ignored, neither as physical nor political subjects.

Conceptually, Hacking develops his thinking further through his concept of 'making up people', which quite literally describes how new types of people come into being through their naming as particular 'types'. As opposed to suggesting that specific categories of people are discovered, due to better information about their existence, Hacking (2002, p. 106) is careful to explain that it is "not that there was a kind of person who came increasingly to be recognized by bureaucrats or by students of human nature, but rather that a kind of person came into being at the same time as the kind itself was being invented." Things, such as ideas, objects and scientific protocols, can also be brought into existence in this manner, but Hacking is careful to distinguish things from people, emphasizing that people, as autonomous agents, respond to and are changed by their naming. "Making up people", Hacking suggests, "changes the space of possibilities for personhood" (ibid, p. 107), whereas things do not, and cannot, interact with the names that are applied to them.

Taken together, Hacking's notion of risk and his concept of 'making up people' might equally be thought of in terms of 'making up problems' or 'making up risks'. This is because the naming of a person or a thing as a 'problem' or a 'risk' (indeed, the naming of any 'new' entity, irrespective of how it is qualified) opens up new space for thought and action that did not, and could not, exist prior to their naming. In this way, as new concerns and anxieties about crime, disease and terrorism, indeed an infinite number of "non-existent yet possible events" (Power 2013, p. 6), are voiced, one might observe a simultaneous emergence of problems and risks that demand action on the part of diverse institutions, including law enforcement, public health, military, and many others. As Wilkinson (2010, p. 25) observes: "Once labeled as 'risk', problems are framed with a sense of urgency that issues a demand for political attention and moral response." And, while this outcome (a new 'risk' comes into being) is not dissimilar from the outcome advanced in securitization theory (a new 'security threat' comes into being), it is with view to routine 'risk-oriented practices' (Power 2013), and not exceptional circumstances or singular 'speech acts', that this outcome is possible.

As a way of conceptualizing the performative impact of risk – when conceived as a label or category that is used to classify people or things as particular kinds of social problems – Hacking's 'making up people' goes a long way towards shedding light on how new entities might enter into the realm of regulation and be made the subject of risk assessment and management. In contrast to securitization theory, this approach neither marginalizes the physical nor ignores the social, but rather provides space for both the 'real' and the 'constructed' (Hacking 1999). Nor does this approach privilege the words or actions of political elites; nor does it speculate as to their motives. If anything, Hacking's research is most compelling in that it sheds light on how a seemingly mundane, bureaucratic activity – municipal statistics – came to play an instrumental role in bringing new categories of people and things into the domain of political deliberation.

Before proceeding, one further resonance between Hacking's theoretical position and the wider risk literature in sociology merits emphasis. Namely, Hacking's (1990, p. 4) description of risk as the "philosophical success story of the twentieth century" is indicative of a view shared by risk scholars coming from diverse theoretical positions. Namely, it is widely held that risk perception is integral to modern life (see, among others, Ewald 1990; Castel 1991; Beck 1992; Luhmann 1993). Indeed, by some accounts, it is all but impossible for modern society to consider the future through anything other than the conceptual and normative lens of risk (Castel 1991; Luhmann 1993). In this light, while governmentality theorists (for example, Dean 1999) may be critical of Beck's (1992) ontological treatment of risk (a subject I will return to in the following section), there is little disagreement that notions of risk are a pervasive feature of modern life. On the contrary, today it is widely agreed that, "there is scarcely a social problem that is not dealt with in terms of risk" (Ewald 1991, pp. 152-153) and that notions of risk pervade all aspects of individual and collective experience, shaping the conduct of individuals, families, communities and states. In regulatory contexts, this observation is evidenced by a growing number of problematic issues that have come to be framed as 'risks', including "financial well being, human health, safety, environmental quality [and] national security" (Graham 2010, p. 238).

2.3 Problems of measurement

Although an important starting point for critical reflection, understanding how labels and categories contribute to bringing new problems and risks into being tends to be of limited interest to sociologists. As O'Malley (2004) suggests, the naming of new risks has become such a common occurrence that drawing an audience's attention to the fact is almost (although by no means entirely) unnecessary, and, thus, it is rarely the subject of protracted debate. Instead, it is at the level of measurement (or 'assessment', as it is more commonly referred to in the context of 'risk analysis'),[14] and especially at the perceived limits of *rational measurement*, where much of the debate (both academic and technical) concerning contemporary risks resides. It is here that questions of 'limit', namely the limit of scientific knowledge to render an 'objective' assessment of potential harm, come to the fore. Some of the common questions generated in this debate resemble the following: Can the likelihood and consequences of risk 'x' be objectively assessed? If risk 'y' cannot be objectively assessed, what alternative techniques should be deployed? What are the implications of using more speculative (non-quantitative) varieties of risk assessment? In brief, much of the debate concerns what should count as 'objective risk' and as 'objective assessment', where 'objective' underlines a scientific rationality based on quantitative calculation, as opposed to subjective expectations, professional judgments, speculation, rules of thumb, and other non-quantitative modes of calculation (O'Malley 2000, 2003, 2004).

The significance of 'objective risk', as opposed to what one might call 'subjective risk' or 'speculative risk', might best be explained with reference to the 'traditional' risk assessment model, a model that serves as a common reference point for risk experts and risk scholars alike.[15] According to this model, risk is equal

---

[14] 'Risk analysis', traditionally defined as a technical procedure combining 'risk assessment' and 'risk management' (and sometimes 'risk communication'), can broadly "be understood as an overlapping family of methods for the calculation and measurement of risk based in the statistical sciences" (Power 2007, p. 13).

[15] There are many instances of the risk theorists discussed in this chapter drawing on 'quantitative risk assessment' to provide a baseline for their argumentation. Here are just a few examples: "By prevention in this context we mean quite generally preparing for

to the likelihood of an event occurring multiplied by the likely consequences (level of financial loss, extent of environmental damage, number of casualties, and so on) of the event were it to occur. In this context, risk is a *value* (as well as a *means of valuation*) expressed as a *probability*, and of course (according to the model) it is *calculable*. Commonly known as 'quantitative risk assessment', this model represents, above all, "a technical ideal of risk" and its measurement (Power 2007, p. 70), underlining the belief that risks exist as "objective facts that can be explained, predicted, and controlled by science" (Bradbury 1989, p. 381). As Jasanoff (1993) argues in relation to science policymaking, this view of risk (if contradicted in practice) is distinctive of the dominant 'culture' of risk analysis. More generally, Michael Power (2007, p. 70) suggests, it exists "at the centre of the risk management collective imagination, defining a broad community of specialists united in the belief that managing risk demands [quantitative] measurement."

While numerous scientific and technical domains are characterized by their (ostensible) use of 'quantitative risk assessment', the case of insurance has traditionally been credited with significant advancements in probability theory and frequently serves as an anchor point for theoretical discussion in the risk literature (O'Malley 2003). According to François Ewald (1990, 1991, 2000, 2002), insurance has, since the nineteenth century, represented the foremost 'risk technology', one indicative of a worldview patterned on scientific facts and systematic standards of measurement. The subject matter of insurance is that of common, recurring events (for example, car accidents) – phenomena that can be normalized through statistical calculation. In the world of insurance, Ewald suggests (1990, p. 143), "numbers by themselves create meaning" and the logic of probability and statistics ("techniques of objectification") (ibid, p. 144) enable sense to emerge from an "undifferentiated

---

uncertain future losses by seeking to reduce either the probability of occurrence of losses or their extent" (Luhmann 1993, p. 29); "Risk is the measure of an expectation – a mathematical expectation that, according to Pascal is the product of the probability of the event multiplied by its value" (Ewald 2000, p. 369); "This then also means that the boundaries of private insurability dissolve, since such insurance is based on the fundamental potential for compensation of damages and on the possibility of estimating their probability by means of quantitative risk calculation" (Beck 2002, p. 41).

mass of data without any need for reference to a world outside that of pure surfaces and pure factuality" (ibid, p. 143). In this light, the notion of 'risk' departs from its everyday usage as a signifier of a threatening future event, becoming, instead, an analytical tool or means of measurement. As Ewald (1991, p. 207) eloquently writes: "To calculate risk is to master time, to discipline the future." The future (to the extent that Ewald's statement is perceived to be true) can be colonized, its unruly aspects tamed, and decisions made in accordance with a scientific rationality.

However, some events (for example, nuclear reactor accidents) – risk phenomena that are neither common nor readily 'calculable' within the empirical constraints of the traditional risk assessment model – are perceived to be incompatible with the logic of insurability. Specifically, problems of measurement are perceived to arise when a risk calculus premised upon the availability of scientific knowledge threatens to break down in the face of extreme uncertainty. In such cases, the future is perceived to become untethered from a scientific rationality that claims to be based on objective knowledge about the world, and which seeks to inscribe this knowledge in the medium of probability. What if, for example, one does not know the starting parameters called for in the model? What if such an event has never occurred before, so there is no known likelihood of the event occurring in the future, and no knowledge of the likely damage that would arise if the event were to occur? In particular, when it comes to the very worst-case scenarios – the potential catastrophe, the disaster – little is known, and perhaps nothing can be known, about the event. It is at this point that Ulrich Beck's (1992) notion of *incalculable risk* rears its head and creates much disagreement and debate, as the objective rationality of the traditional risk assessment model is cast in doubt, as is the credibility of the scientific and technical experts who continue to claim it works.

2.3.1 'Risk society' and the 'special case of high technology'

For Ulrich Beck (1992), the existence of 'incalculable risks' is a defining feature of contemporary life. In his influential thesis, *Risk Society*, Beck describes a "modernization process" that has led to the unintended production of self-produced risks "before which the human imagination stands in awe" (ibid, p. 20).[16] The "*wholesale product* of industrialization" (ibid, p. 21, emphasis in original), these risks are described as having "a new quality", namely, they are global in nature and have consequences that may extend over indefinite periods of time (ibid, p. 22). Above all, it is with a view to "techno-scientifically produced risks" (ibid, p. 19), such as radioactivity, toxins and pollutants, that Beck argues that the world today is no longer only threatened by finite risks to individuals and communities, but also to catastrophic dangers to "all life on Earth" (ibid, p. 21). For Beck, this represents a qualitative change, one that is indicative of "a real transformation in society" (ibid, p. 20), which must now confront risks that are, by their very nature, beyond "[t]he normative basis of their calculation" (ibid, p. 22). That is, they are incommensurate with the traditional risk assessment model, and, in turn, "unpredictable, uncontrollable and ultimately incommunicable" (Beck 2002, p. 40).

In essence, Beck's 'risk society' is confronted by risks that are, in fact, no longer 'risks' at all, but rather incalculable dangers, for which, Beck contends, there is no 'objective' measure. To put it another way, such risks are said to be uninsurable. That is, they are beyond the capacity of insurance to calculate potential loss, and thus beyond setting premiums and beyond indemnification (an argument made by Dean 1999 and O'Malley 2000, 2003 in their critiques of Beck). While Beck does not suggest that these conditions have led to a world where risk assessments are no longer conducted, much less that scientific and technical experts no longer claim to possess the necessary knowledge to do so, he does claim that efforts to 'rationally' assess so-called 'modernization risks' represent an attempt to "*feign control over the uncontrollable*" (Beck 2002, p. 41, emphasis in original). Quite literally, Beck suggests, how, and why, would an insurer (or, for that matter, a risk

[16] See, also, Giddens (1990). Like Beck, Giddens argues that society is confronted by risks that are the direct and material consequence of scientific progress.

analyst, a scientist, a politician or anyone else) attempt to empirically evaluate a catastrophe when the basic means of valuation required to evaluate that catastrophe does not work? This question points to an unnerving realization for Beck (1992, 2002, 2009), namely: those who do claim to know, at least within the prescribed scientific rationality of the traditional risk assessment model, are, at best, mistaken, and, at worst, deliberately misleading others. In such cases, Beck suggests, risk assessment, and trust in scientific expertise, is undermined.

Like Beck, Niklas Luhmann (1993), although coming from a different theoretical background, also places considerable emphasis on the destabilizing effects of advances in science and technology and attempts to make a distinction between 'predicable risks' and 'unpredictable dangers'. In particular, Luhmann (ibid, p. 83) emphasizes "the special case of high technology", including risks associated with "rapid technological developments in fields under the scientific aegis of physics, chemistry, and biology." According to Luhmann (ibid.): "More than any other single factor, the immense expansion of technological possibilities has contributed to drawing public attention to the risks involved." Also like Beck, Luhmann (ibid, pp. 113-114) points to a loss in confidence in those who claim to possess the necessary knowledge to anticipate and prevent unpredictable dangers, emphasizing that, "[u]nder certain conditions, above all the conditions of risky technologies, confidence in the self-confidence of others evaporates." In the case of the most improbable events, Luhmann suggests, "tenable consensus" is no longer possible and "efforts to base decisions on rational calculation not only remain unsuccessful, but in the last instance also undermine the claim of method and procedure to rationality" (ibid, p. xxx). "This means that politics cannot rely on the quantitative calculation of risk … Instead it has to make do with informal guesses" (ibid, p. 15). However, unlike Beck, as O'Malley (2004) points out, Luhmann's position does not centre on statistical prediction, but rather on causal predication, proposing that risks can be attributed to 'decisions made' and dangers can be attributed 'externally' – that is, to sources beyond our control.

2.3.2 Uncertainty and the will-to-order

While Beck is not alone in his suspicion that certain contemporary risks, including those associated with technological advancements and (a more recent addition to the 'risk society' thesis) 'global terrorism' (Beck 2002), challenge a risk model founded on the presumption of empirical evidence, Beck's grand claim – that we are living in a 'post-risk-calculation' or 'post-insurance' age – is contested. As Nikolas Rose (2002, p. 213) argues: the "notion of risk society, though suggestive, is misleading. It implies something homogenous and all embracing, an array of effects that are amenable to an epochal sociological explanation." In practice, Rose suggests, risk (and its measurement) cannot be defined *en masse*, as it does not conform to a singular type, rationality or technique. Rather, risk is as varied as the venues within which it is observed and measured, conditioned by localized approaches to dealing with uncertainty. In brief, risk, and 'risk thinking', is heterogeneous: "It may be clinical, epidemiological, actuarial, forensic, probabilistic, and much else besides" (ibid.). Moreover, and in stark contrast to Beck, Rose underlines that, irrespective of the ontological status attributed to cotemporary risks, as well as the perceived 'limits' of 'traditional' risk assessment techniques, concerted efforts are regularly being made to 'calculate' the seemingly 'incalculable'. According to Rose:

> "The incompleteness, fragmentation, and failure of risk assessment and risk management is not a threat to such logics, merely a perpetual incitement for the incessant improvement of systems, generation of more knowledge, invention of more techniques – all driven by the technological imperative to tame uncertainty and master hazard." (2002, p. 228)[17]

For Rose, and governmentality theorists more generally (Dean 1999; O'Malley 2003; Erickson and Doyle 2004, among others), the point of conflict with Beck's 'risk society' thesis is not the question of whether the future is uncertain (and possibly getting more so by the day). What is, however, is the question of whether

[17] An observation that is closely echoed by Dean (1999, p. 191), who suggests that the failure of risk assessment "(itself judged through a particular epistemological framework) does not mean the abandonment of the attempt to construct coherent programmes of government. Rather, its discovery is an incitement to the problematization, reformation and replacement of such programmes."

individuals and populations are presently confronted by dangers that are beyond legitimate reflection and action. As Pat O'Malley (2003, p. 277) concedes: "It may be that '[r]isk society is a catastrophic society' (Beck 1992: 24), but this does not mean that alternative forms of calculation cannot govern such developments." As Rose's critique suggests, sites of risk selection, and modes of risk assessment, are in fact plural, diverse and *diversifying*. In turn, this diversification suggests the possibility of 'new' approaches to dealing with uncertainty, beyond the traditional risk assessment model – a model that has tended to dominate both technical and theoretical discussions on the subject of risk. Indeed, even in the case of insurance, traditionally "regarded as the archetype of modernist governance of the future" (O'Malley 2003, p. 275), Erickson and Doyle (2004) have shown that heightened perceptions of uncertainty have, for the most part, not dissuaded insurers and reinsurers from tackling such diverse 'problems' as earthquakes, hurricanes, terrorism and corporate fraud liabilities (ibid, p. 20). Rather, these so-called 'catastrophe risks' have motivated insurers to generate creative 'solutions' to these problems in pursuit of profitable insurance products (choices that depend upon each insurer's own 'appetite for risk') (ibid.). Some insurers, they suggest, are willing to provide insurance coverage even in the absence of "meaningful statistics", adopting an approach to risk assessment akin to 'gambling' – relying as much on gut feelings and intuition as hard 'facts' about the world (ibid, p. 18).

In regulatory contexts, it has similarly been shown that, while quantitative methods remain an idealized mode of decision-making, as they suggest the possibility of 'objective' or 'value-neutral' policy decisions, other conceptual frameworks are commonly deployed to arrive at informed policy choices. For example, as the authors of one report for the Organisation for Economic Co-operation and Development (OECD) suggest, when regulators are confronted by "complex policy issues", cases where uncertainty cannot be "assumed away", decision-making may be structured according to a 'procedural rationality' "within which the different components of the decision problem can be separately analysed, and then put together in a consistent way" (OECD 2010, p. 129). From the perspective of regulators, "in a world where transparency and accountability are

viewed as necessary conditions of legitimacy", what is important is that decision-makers are as "explicit as possible about the steps which led them to their final determination" (ibid.). Or, as Power (2007, p. 155) suggests, the very notion of "risk management as a category has changed its meaning and expanded its scope well beyond its technical foundations", with risk managers shifting towards the development of regulatory frameworks that empathize 'process' and 'transparency' over formal calculations based on quantitative risk assessment.

Moreover, Majone (2010), and others (for example, O'Malley 2004; Graham 2010), call into question the very notion that there exist distinct situations where the level of scientific knowledge is sufficient to permit 'quantitative risk assessment' and situations where scientific knowledge is insufficient, thus requiring informal, 'qualitative' methods. "In reality," Majone (2010, p. 108) suggests, "these are two points on a knowledge ignorance continuum rather than two qualitatively distinct situations." This leads Majone (ibid, p. 109) to conclude that, "a sensible principle of decision making is one that uses all the available information, weighted by its reliability in terms of subjective probabilities, instead of privileging some particular risk." With a view to "progress in the decision sciences," including Bayesian statistics, which treats "strength of belief as an indication of probability" (Graham 2010, p. 242), Graham (ibid, pp. 241-242) similarly argues that Knightian[18] distinctions between "'risk', where probabilities of adverse events are known or ascertainable based on actuarial data, and conditions of 'uncertainty', where probabilities of adverse events are unknown" are "no longer meaningful."

In the case of 'regulatory science' or 'science policy', a context where "the normal state of affairs is neither scientific certainty nor complete ignorance" (Majone, pp. 108-109), this observation is especially apparent. As Jasanoff suggests (1990, p. 14), regulatory science invariably "straddles the dividing line between science and policy", on the one hand attempting to furnish rigorous scientific evidence and risk estimates to support policy decisions and on the other having to make these decisions on the basis of less than perfect knowledge. Based on her

[18] The American economist Frank Knight is typically credited with distinguishing between 'measurable risk' and 'unmeasurable uncertainty' (Knight 1921).

research on scientific advisory committees in the United States, Jasanoff describes regulatory science as a "hybrid" activity that "combines elements of scientific evidence and reasoning with large doses of social and political judgment" (ibid, p. 229). Rather than strict adherence to quantitative methods, what Jasanoff's (ibid.) research demonstrates is that regulatory science invariably mixes facts and values in pursuit of particular regulatory goals. In this context, risk estimates can be understood as the outcome of a negotiated process that attempts to carefully balance competing demands and interests, while drawing on standards of measurement that are at once scientific and political (ibid.).

Occupying a 'grey area' between science and politics, regulatory science (and risk assessment itself) has been described as "a classic 'trans-scientific' activity carried out by regulatory agencies" (Jasanoff 1990, p. 216) seeking to develop "'techniques, processes and artifacts' that further the task of policy development" (ibid, p. 77). According to Alvin Weinberg (1972, p. 209, emphasis in original), who coined the term 'trans-science' in the early 1970s: "Many of the issues which arise in the course of the interaction between science or technology and society … hang on the answers to questions which can be asked of science and yet *which cannot be answered by science*." Under these conditions, Weinberg suggests (1985, p. 68), regulatory science has emerged as a new branch of science, one "in which the norms of scientific proof are less demanding than the norms in ordinary science." In other words, regulatory science "falls on the practical side" of the division between so-called 'pure' and 'applied' research (Jasanoff 1990, p. 77). In light of disagreements between experts on the 'correct' interpretation of policy issues, calling into question the "scientistic and separatist view of science in the policy process" (Irwin et al. 1997, p. 19), regulatory science effectively bridges the gap between 'uncertainty' and 'risk', enabling regulatory decisions to be made in the absence of secure knowledge about the world. In brief, "regulatory science is concerned with how science can make predictions on the basis of uncertainties" (ibid.).

While 'regulatory science' ('trans-science' or 'science policy') can be meaningfully contrasted – as an 'ideal type' (Jasanoff 1995) – with so-called 'ordinary science', it is nonetheless more heterogeneous than Weinberg's (1972)

formulation of the concept would suggest (Irwin et al. 1997). Specifically, it is questionable whether it is possible to determine "where science ends and trans-science begins" (Weinberg 1972, p. 216). In practice, as Jasanoff (1987, p. 211) observes, "the scientific and technical aspects of decision-making" cannot "be isolated from the socio-political ones." Indeed, it has been suggested that it is precisely with a view to regulatory science's 'heterogeneous and hybrid character' – involving a range of academic disciplines, drawing on diverse risk assessment techniques embedded in varied institutional and national contexts (Irwin et al. 1997) – that one is able to discern the sheer diversity of ways in which regulatory subject matter are made amenable to risk assessment and risk management. In this light, the search for singular 'types' of risk, which can be evaluated on the basis of science alone, is not only an oversimplification, but also fails to capture the inherent variation that characterizes risk and regulatory processes. "The lines between science, policy, and the areas where the two are mixed", Jasanoff (1987, p. 224) argues, "are difficult to draw not merely because science is indeterminate, but because the effort to make such distinctions is politically charged."

Far from being exceptional, regulatory science routinely confronts questions about risks (ranging from GM crops to nuclear reactor accidents) characterized by "intrinsic, irreducible uncertainty" (Majone 2010, p. 99). Indeed, it is precisely these sorts of contingencies – "emerging risks that are scientifically uncertain, economically significant, and politically sensitive" (Graham 2010, p. 245) – that are of particular concern to national governments, motivating regulatory processes that, on the one hand, acknowledge the 'limits' of scientific knowledge, and, on the other, strive to produce risk estimates based on styles of reasoning that continue to appeal to the idealized standards of science and the possibility of 'objective' risk assessment (Jasanoff 1987, 1990). In other words, even in the absence of 'hard' evidence about highly uncertain risks, there remains an enduring belief that risks can be 'calculated', and, moreover, that science can provide the necessary ingredients for doing so. Moreover, for the scientific and technical experts consulted for their specialist knowledge, it is in their interests to shift the boundaries of analytical attention towards 'objective' science and away from 'subjective' politics,

valorizing the importance of scientific expertise in policy processes (ibid.). In turn, it is with a view to this accomplished 'boundary work' that one can gain a more nuanced understanding of the 'micro-world' of risk analysis, a world built upon not only scientific standards of measurement, but also on an active politics undertaken to legitimize and sustain the authority of science itself (Jasanoff 1993).

As the above discussion suggests, there exist a wide variety of techniques that can be (and, indeed, *are*) deployed to estimate risk, beyond the perceived 'limits' of 'quantitative risk assessment'. Accordingly, a growing number of risk scholars argue that new space should be made for the governmental analysis of alternative approaches to risk measurement, including more speculative varieties of assessment based on estimation, imagination, and forecasting (Erickson and Doyle 2004; O'Malley 2000, 2003, 2004), as well as 'procedural' or 'process-based' approaches that are indicative of "a distinctive kind of organizational proceduralization which prioritizes the auditability process" (Power 2007, p. 180). As O'Malley (2000, p. 466) suggests, while such approaches may be "less formal and calculable, perhaps more lay or commonsensical", they need not be less "'rational'". Thus, while 'risk society' theorists may view such 'uncertain techniques' (as opposed to 'risk technologies') critically, as they fall outside the remit of statistical calculation, they nonetheless constitute legitimate efforts aimed at applying order to disparate elements of an unknown future. From the perspective of governmentality theorists, the very adaptability of risk rests in the fact that it is, above all, a category of understanding, "a schema of rationality, a way of breaking down, rearranging, ordering certain elements of reality" (Ewald 1991, p. 199). In other words, as Ewald (1990, p. 142) succinctly argues, "anything can be a risk – everything depends on the way the danger is analyzed and the potential event is evaluated."

In sum, risk measurement would appear to be more adaptive than 'risk society' theorists would contend, and there remains considerable scope for empirical research that focuses on sites of risk assessment and risk management that move beyond 'meaningful statistics'. Yet, what does it mean to move beyond 'objective risk' and 'objective risk assessment'? What techniques fall within the scope of 'speculative risk'? How are these techniques used, and to what end? These

questions offer a new problematic for critical reflection and debate. For François Ewald (2002, p. 288), who has (as discussed above) played a significant role in the conceptual framing of insurance risk – a technology of risk that prizes the virtues of the scientific method and scientific reason – 'new' approaches to risk presuppose "a new relationship with science and with knowledge." And, while such approaches do not appear to abandon much of the language of risk, they nonetheless seem to invite "one to anticipate what one does not yet know and to take into account doubtful hypotheses and simple suspicions" (ibid.). For some, these are unfamiliar (even unsettling) conceptions of risk, as risk has, for some time, been interconnected with the promise of science to order the heterogeneous elements of an uncertain future, where now such potential is increasingly in doubt.

2.4 Anticipatory government

Risk also takes on another configuration, where it is neither conceived as a signifier of potential danger nor as a means of measurement, but as a means of *decision-making* in the face of an uncertain future. In this context, risk is said to enable action in the present in an attempt at minimizing anticipated harm (and providing an ostensibly 'rational' basis for a variety of regulatory choices). Whether this anticipated harm is perceived to be minimal or catastrophic, imminent or on the far horizon, and, indeed, *calculable* or *incalculable*, to act on risk, and through the logic of risk, is a defining characteristic of modern life (Dean 1999; Rose 2002; Power 2004). This is because, to acknowledge risk, to measure it – either through the rigor of the scientific method or through the vicissitudes of pure imagination – is to make risk real, to give it form, which, in turn, necessitates a decision by a decision-maker; even if that decision is to do nothing. To do otherwise would be unacceptable; as to know something about the future and yet remain idle is incompatible with today's risk-aware and risk-averse society. In the realm of politics, the historian of science, Susan Wright (2007, p. 103), describes this modern contract with risk as "an insurance policy for political reputations". It is, then, through its capacity to mobilize, to enable action in the name of prudence, that risk most clearly reveals

itself as a practical instrument of government. In the following, I will discuss the work of theorists who have traced out the origins of this modern contract, as well as the ways in which they suggest it is adapting to permit those potentialities – those dangers associated with modernization itself – that would seem to be beyond rational measurement and control, and thus beyond government.[19]

2.4.1 Three faces of prudence

Drawing on the work of François Ewald provides a glimpse of how risk, as an instrument of government, has come to occupy the space it does in the early twenty-first century. Specifically, Ewald (2002, p. 296) describes "three attitudes with regard to uncertainty" that have emerged since the nineteenth century, and which have accompanied society's changing conception of the future and how one might intervene in the present to prepare for that future. Ewald conceives of these three attitudes, or "three faces of prudence" (where Ewald takes prudence to mean "behavior in the face of uncertainty"), in terms of providence, prevention, and precaution (ibid.). Importantly, Ewald does not suggest that these three behaviors in the face of uncertainty are incompatible or that the emergence of one spelled the end of the other two (as 'risk society' theorists would contend), but rather that "[e]ach has its field of competence and area of validity" (ibid.). Exploring these three faces of prudence in greater depth is revealing of the ways in which risk is mobilized in response to varying perceptions of uncertainty, and how such uncertainty is negotiated and managed in an effort to mitigate potential harm.

The nineteenth century, Ewald (2002, p. 293) suggests, was one concerned with providence, "linked to notions of fate, chance and misfortune, and hazard", as well as that of prudence, which required that individuals take responsibly for their

[19] Conceptually, it is important to emphasize that my use of the word 'government' in my thesis (unless qualified more precisely, for example, 'national government', 'government agencies', and so on) is not intended to refer to a centralized state government or sovereign authority. Conceptually, and in keeping with the governmentality literature, the term 'government' (and its derivatives) is intended to capture multiple governmental actors and organizations engaged in the 'government of conduct' (Rose 2000).

own destiny. “The world of providence”, Ewald writes, “is one in which one must recognize his or her own weaknesses and fragility, subject to incessant reversals of fortune; it is a world of chance events … where one knows oneself to be vulnerable and scarcely hopes to use science and engineering (which are not readily available) in order to rebalance one’s relationship with nature” (ibid, p. 276). In this context, each individual is said to be responsible for his or her own conduct, where their security depends wholly on their capacities to avert injury and their provisions to compensate for potential loss. The fault of misfortune (unless intentionally imposed by another) rests solely with them, as do the costs. Although providence is said to mark the beginning of an active relationship not only with the present but also with the future, it is a future that is scarcely foreseeable and beyond control, and thus beyond the remit of calculable risk and prevention. At the same time, the potential damages arising from human error are envisioned as finite, and are thus the responsibility of individuals and not society as a whole.

By the late nineteenth century, Ewald suggests, notions of risk, and its management, began to enter into the daily lives of individuals, spurned by a form of solidarity in response to common workplace accidents, where faults were considered “less as individual than organizational” (Ewald 2002, p. 281). Individuals came to be viewed as links in a technical system, more than free agents. Compensation through insurance provided a safety net for workers, and minimizing the likelihood of harm became a preoccupation for employers. Advances in insurance risk, in turn, elevated the science of statistics, permitting the future to be known more and more through the medium of probability. In this context, Ewald suggests, the notion of prevention replaced that of providence, becoming a staple of modern society, where prevention, “presupposed science, technical control, the idea of possible understanding, and objective measurement of risks” (ibid, p. 282). Throughout the twentieth century, faith in the mastery of science over uncertainty grew exponentially, tied to perceptions of a “scientific utopia ever more capable of controlling risks” (ibid.). In this fashion, Ewald describes an expanding realm within which technologies of risk became the preferred tool for dealing with all manner of

potential hazard, from 'occupational hazard' to 'social risk' to 'environmental risk'; up to the perceived limits of Beck's 'society of risk' (Ewald 2000).

However, by the end of the 1970s, Ewald (2000) suggests, environmental concerns began to suggest a future not only populated by localized accidents but also by the possibility of global catastrophes. At this point, a risk calculus intended for the valuation of finite harms that can be reasonably predicted and their impact mitigated appeared to reach its limits. In this context, Ewald (2002, p. 292) suggests, the utopian ideal of 'preventable risk', where decisions can be made based on what is more or less probable or improbable, gave way to precaution, where "decisions must be made by reason of and in the context of scientific uncertainty." Precaution, then, is said to mark the limits of risk (or, more precisely, technologies of risk) and its perceived capacity to render the future knowable, "[returning] us to an epistemology of the relativity of scientific knowledge" (ibid, p. 288). For Ewald, this suggests the possibility of "a risk beyond risk", for which one does not have, and cannot have, the "knowledge or the measure" (ibid, p. 294). Yet, far from collapsing the enterprise of prudence, due to insufficient knowledge about the future, such extreme uncertainty is said to call for even greater caution, which, if fully realized, imagines the worst-case scenario or "worst imaginable accident" (Dean 1999, p. 183) and prepares for that contingency (Cooper 2006; Furedi 2009). In this sense, precaution invites a new form of responsibility in the face of unforeseeable hazards. Unlike the responsibility imposed by providence in the nineteenth century, which responded to finite damages facing individuals, the responsibility imposed by precaution is total, as the potential damages are assumed to be irreversible and global. In those cases where the logic of precaution is believed to be justified, the only acceptable outcome or event is no event at all, as its potential costs cannot be borne by society, and thus the event must be pre-empted.

2.4.2 Configurations of risk and uncertainty

Although Ewald's three 'faces of prudence' offer a useful schematic for thinking about different approaches to decision-making in the face of uncertainty, there is a

risk in drawing too sharp a distinction between them, as well as in limiting one's analysis of risk to these modes of decision-making, as there are no such constraints on risk management in practice. In practice, O'Malley (2004, p. 7) argues, managing risk takes on diverse and heterogeneous forms that are "constantly being tinkered with, re-imagined, reinvented, [and] 'improved'". For example, in the case of 'catastrophe insurance', speculative and probabilistic techniques are increasingly developed and deployed side-by-side (Ericson and Doyle 2004; O'Malley 2004). Therefore, while Ewald (2000, p. 296) acknowledges (as noted above) that there exists space for providence, prevention and precaution, his suggestion that they be kept separate, respecting "their spheres of influence and jurisdiction", is not something that can necessarily be achieved in practice, as governing through risk (in any given context) is likely to be irreducible to a discrete technique (say prevention or precaution). Instead, it is more likely to be made up of multiple ways of responding to the problem at hand. Therefore, O'Malley (2004, p. 24) suggests, it is both more practical, and more reasonable, to "envision governmental technologies in terms of variable configurations, assemblages or ensembles of elements, rather than as fixed types".[20] Accordingly, O'Malley (ibid.) proposes thinking in terms of specific 'configurations' of risk and uncertainty, which leaves room for 'hybrid' forms of risk and risk management. This thinking, in turn, permits an 'analytics of government' that allows meaningful distinctions to be made between (calculable) risk and (incalculable) uncertainty without requiring that complex assemblages be reduced to either 'objective' or 'speculative' modes of government.

More than the differences between providence, prevention and precaution, it is their similarities that are most suggestive of their shared capacity to enable action in anticipation of potential harm. That is, irrespective of whether future events are imagined as calculable or incalculable, amenable to prevention or merely precaution, each attitude towards uncertainty, as well as the various 'technologies of risk' and 'uncertain techniques' it is bound up with, is concerned with governing

[20] An observation that is closely echoed by Dean (1999, p. 178), when he suggests that risk should be "analyzed as a component of assemblages of practices, techniques and rationalities concerned with how we govern".

through "reasoned estimation of an indeterminate future" (O'Malley 2004, p. 6). The significance of this observation should not be underestimated. The reason being, much of the recent critique of contemporary risk management implies that precautionary risk signals a departure from statistical forms of risk assessment, and, in turn, a departure from meaningful forms of risk management. This is most evidently reflected in the work of 'risk society' theorists, who claim that we are presently living in an era of 'post-risk-calculation',[21] but also, as O'Malley (2004) points out, it appears, albeit less frequently and to a lesser degree, in the work of some governmentality theorists, including Ewald, in as much as they suggest that there exist discrete cases of catastrophic risk that are similarly beyond calculation and control. Yet, as noted previously, while it is certainly true that there exist cases that do not lend themselves to the probabilistic model of 'informed' decision-making, this is not to say that decisions about such cases are not 'informed', merely that they are informed by other metrics, such as "experienced judgment, shrewd guess work, rules of thumb, analogies, and so forth" (O'Malley 2004, p. 13).

Of course, whether such alternative (that is, non-probabilistic) approaches to risk management will 'work' – capturing a 'true' picture of future realities that can be responded to in 'successful' ways – is another question, but a question for which, O'Malley (2004) argues, sociologists are not best suited to answer. For the purposes of a governmental analysis of risk, he suggests, it is enough to acknowledge that there exist diverse ways of imagining the future, all of which inform decisions in the present, and all of which can claim (in their own right) to be legitimate ways of doing so. The challenge, then, is not to correctly discern the 'best' way to govern, but to acknowledge those ways in which such diverse problems as climate change and terrorism are *already* being governed (ibid.). Indeed, even in the case of 'precautionary risk', often portrayed as beyond 'rational' response, there exists the possibility of highly specific forms of measurement and intervention. After all, as O'Malley (ibid.) points out, precautionary responses are responses to those

[21] See Dean (1999, p. 182) for a more extensive critique of Beck's methodological approach to risk, which he suggests reflects the ontological belief that "real riskiness has increased so much that it has outrun the mechanisms for its calculation and control".

imaginable catastrophes that would seem to be beyond compensation. In each case, it should be recalled, anticipations of the future can only exist as *representations*, as imperfect as these may be. It should also be noted that precaution does not only motivate inactivity, as often suggested, but it can equally motivate, as the sociologist Melinda Cooper (2006) argues with respect to the threat of terrorism, rigorous action in the form of counter-proliferation, surveillance, emergency preparedness, and alike.[22] In brief, risk, either 'objective' or 'speculative', statistically calculated or discerned through crude estimation, informs prudential practices. It is, in turn, by way of attending to these practices that one is provided with evidence of how risk, in specific contexts, is applied to the management of specific problems.

2.4.3 The management of regulation

In an effort to situate 'risk management' more concretely in the context of 'regulatory governance', additional historical context is valuable. Specifically, since the 1980s, largely "in response to criticisms about the emergence of the so-called 'regulatory state' and corresponding concerns about over-regulation and 'burdening industry'" (Hutter 2005, p. 1),[23] 'risk-based' frameworks have come to be favored by regulators and applied to an ever-larger array of regulatory activity (Hutter 2005; Black 2010; Fisher 2010; Graham 2010). Characteristic of the so-called 'new public management', the use of 'risk-based tools' – especially 'quantitative risk assessment' (Bounds 2010) – are intended to reflect 'styles of management' visible in the private sector, including greater attention to reducing "the costs of regulation" (Hutter 2005, p. 1). Holding the promise of enhanced 'objectivity' and improved 'transparency', risk-based frameworks suggest both the possibility of greater regulatory efficiency, and offer regulators a means of providing a more explicit accounting of their decision-making activities in the hope of averting criticism for doing too little (type 1 errors) or too much (type 2 errors) to regulate (Hutter 2005;

[22] See, also, Aradau and van Munster (2007, 2008) and Furedi (2009).
[23] Hutter's (2005, p. 1) analysis primarily focuses on the so-called 'regulatory crisis' in the UK context, but also underlines comparable developments in the US under Regan, as well as other "advanced industrialized societies" during the 1980s/1990s.

Black 2010; Bounds 2010; Majone 2010). At the same time, the vocabulary of 'risk', 'risk assessment' and 'risk management', as well as other 'risk regulatory concepts',[24] has become (especially within the last ten years) a "central [feature] of administrative decision making" (Fisher 2010, p. 46), lending "a sense of strategy and control" (Black 2010, p. 188) to regulatory activity. In this manner, the adoption of risk-based frameworks (including the language they are bound up with) has come to be "seen as a functionally efficient tool" (ibid, p. 190) and, in many ways, "a badge of legitimacy" (ibid, p. 189) (see, also, Hutter 2005; Fisher 2010).

Coupled with the adoption of risk-based frameworks to enhance the efficiency of regulatory activity (and to limit the 'reputational' risks to regulators stemming from regulatory failures), the reforms of the 1980s also contributed to the "decentring of the state" to include a much wider variety of actors and organizations in regulatory processes (Hutter 2005, p. 3). Indeed, as Rhodes suggests:

> "[T]here is no longer a single sovereign authority. In its place, there is the multiplicity of actors specific to each policy area; interdependence among these social-political-administrative actors; shared goals; blurred boundaries between public, private and voluntary sectors; and multiplying and new forms of action, intervention and control." (1996, p. 658)

In other words, regulation has become 'fragmented' (Hutter 2005). Significantly, this transition – from state sovereignty to a multiplicity of "systems of rule" (Bunton and Peterson 2005, p. 4) – is said to coincide with the emergence of 'governance', a concept that is often defined as a mode of governing that is primarily shaped by decentralized networks of sub-national, national and international organizations, as opposed to centralized government authorities (Rhodes 1996).

More broadly, 'governance' has been defined as "'the prevailing patterns by which public power is exercised in a given social context'" (Jenkins 2002, p. 485, as citied in Corbridge et al. 2005, p. 153). With a view to this more general

[24] Included under the rubric of 'risk regulatory concepts', Fisher (2010, p. 48) suggests, "are not only concepts of risk, risk management, and risk assessment but associated concepts such as comparative risk analysis, the precautionary principle, risk communication, security, uncertainty and hazard."

understanding of 'governance', it is possible to shed light not only on the range of actors and organizations engaged in regulatory activity, but also on the changing role of regulatory authorities in orienting risk management processes. In particular, it is often suggested that the role of the state has shifted towards facilitating risk management through 'indirect action' – governing 'at a distance' or "steering and regulating rather than rowing and providing" (Rose 2000, p. 324). Manifest in a growing number of formal guidelines and visionary documents outlining 'risk assessment' and 'risk management' procedures, the production of prescriptive guidance offers a new mechanism for shaping regulation (Power 2007; Graham 2010). Promising greater efficiency, it is through such indirect action that regulatory authorities seek to empower an expanding array of governmental actors and organizations, including private enterprise and individuals, to play a more active role in managing risk (Rose 2000; Fisher 2010). At the same time, it promises to shift much of the responsibility for risk management (and potential blame for perceived failures) to a new constellation of actors and organizations.

For some risk scholars, the emergence of 'governance' (as opposed to 'government', as the word is typically conceived in policy arenas) is indicative of a new type of governmentally, one that "reflects a regulatory preference for indirect action and influence by prescribing frameworks and principles and by enrolling self-regulating resources" (Power 2007, p. 37). Indeed, by some accounts (ibid.), attention to the 'management of regulation' – the 'control of control' – has largely displaced the need for direct action on behalf of regulatory authorities. For some, this transformation is said to be at the heart of 'risk-based regulation' (ibid.). Described by Michael Power as "governance of the risk assessment and risk management process" (ibid, p. 19), this so-called "'managerial turn'" (ibid, p. 36) is said to mark "the extension of risk as an organizing category … to the management process itself" (ibid, p. 156). Consequently, in light of a greater accent on management and "the rational design of the risk management process" (ibid, p. 28), Power suggests, "the distinction between regulating and managing has become blurred" (ibid, p. 192). To the extent that a managerial approach to regulation has come to replace (some) of the 'risk-based tools' (Hutter 2005) familiar to 'risk

analysis', "[a] cultural 'trust in numbers'" is said to "have given way to an emphasis on systems and processes to define governance" (Power 2007, p. 178).

While there are other aspects of 'risk-based governance' that could be explored here, including trends in 'upstreaming' citizen engagement (see, for example, Wilsdon 2004; Tait 2009), my intention is simply to underline that 'risk-based' approaches, while diverse, also reflect rationalities[25] that are characteristic of contemporary forms of government. Moreover, it tends to be with a view to 'risk' and 'risk management' that much regulatory activity is currently framed. At the same time, to what extent individual 'risk regulation regimes' or 'regimes of government' prescribe to the technical ideal of 'risk analysis', or whether the language of 'risk' and 'risk management' is intended to play a more rhetorical function, is highly variable. As Hutter (2005, p. 4) suggests, a key factor influencing the degree of adherence to a 'risk-based' approach to regulation is the degree of "buy-in to the risk philosophy". In any case, just as risk assessment, in practice, does not ascribe to an absolute standard, it is perhaps more appropriate to forgo strict classifications of regulatory activity, given that pure 'types' rarely represent reality. Indeed, in any given context, and especially in the context of science policymaking (as discussed earlier), risk regulation exists as a hybrid activity, one that combines formal modes of calculation with various degrees of rhetorical structuring intended to lend a sense of objectivity and control to an uncertain future.

2.4.4 Risk regulation regimes

Ultimately, key to understanding the diversity of ways in which various governmental actors and organizations 'handle' or 'manage' risk is to acknowledge that risk is, above all, 'contingent' or 'context-dependent' (Jasanoff 1993). That is, "what people claim to know about risk is … constructed in different ways in different political and cultural settings" (ibid, p. 127). In light of this variability, Hood et al. (2001, p. 8) suggest, it is necessary for risk scholars "to go beyond

[25] Where I take 'rationality' to mean "any form of systematic or explicit thinking aimed at structuring how things are and how things aught to be" (Dean 1999, p. 11).

generalizing perspectives like 'risk society' to a more disaggregated analysis" of risk domains that can vary widely from one domain to another. In regulatory contexts, they suggest, it is precisely this sort of variation that contributes to an "'archipelago' of risk domains … with very different policy stances", both between and within countries, as well as over time (ibid, p. 6). In the first instance, for example, as Jasanoff (1993, p. 127) has shown, "[c]ountries as similar as the United States and Britain … differ markedly in the kinds of information they deem necessary and sufficient to establish the existence of an actionable risk." In the second instance, Hood et al. (2001, p. 7) observe, considerable variation exists across risk domains within countries, including various approaches to 'standard-setting', which are characterized by different 'cultures' of risk assessment, ranging from 'cost benefit analysis' (road safety) to 'quantitative risk assessment' (nuclear power plant safety) to "qualitative 'seat of the pants' approaches" (gun control).

In an effort to conceptualize this apparent diversity, and to offer "a way of describing, comparing, and explaining" variations between risk domains, Hood et al. (2001, p. 8) propose the concept of 'risk regulation regimes'. Here, "'[r]egime' connotes the overall way risk is regulated in a particular policy domain" (ibid.). In turn, the analysis of various risk regulation regimes, they suggest, should center on the forces that underpin how regimes function (how they 'work' or how they 'fail'), taking into consideration not only questions of "institutional geography and formal rules", but also "the range of risk-assessment techniques and policy-making approaches" that characterize and shape "different fields of risk regulation" (ibid.). Moving beyond "macroscopic" world-historical perspectives on risk, like 'risk society', "which inevitably can deal only in broad-gauge interpretation" (ibid, 14), this approach is intended to "bring out variety that is otherwise hard to see". In this manner, Hood et al. (ibid, p. 16) suggest, "a risk regulation regime approach is not just a tool for analysis – a lens that comes between the microscope and the telescope – but also a challenge for explanation of observed variety."

Variation between risk domains, Hood et al. (2001) argue, contributes to different regime 'anatomies', which can broadly be conceived along two dimensions. The first dimension, they suggest, is comprised of "three components that form the

basis of any control system – that is, ways of gathering information, ways of setting standards, goals, or targets, and ways of changing behaviour to meet the standards or targets" (ibid, p. 21). The second dimension, they suggest, is defined by 'regime context' and 'regime content'. In the first instance, 'regime context' refers to "the backdrop of regulation, comprising, for example, the intrinsic characteristics of the problem it addresses, public and media attitudes about it, and the way power or influence is concentrated in organized groups" (ibid, p. 28). In the second instance, 'regime content' refers to specific "regulatory objectives, the way regulatory responsibilities are organized, and operating styles of regulators" (ibid.). Significantly, Hood et al. (ibid.) argue, these components (among others) shape the 'space' within which risk regulation operates, influencing policy design. In particular, the authors make a strong case for the effect of 'regime context' on 'regime content', drawing attention to the "'inner lives' of regulatory regimes," including "the attitudes, beliefs, and conventions of the various technocratic and bureaucratic 'tribes' in the regulatory machine" (ibid, p. 18).

Having at its foundation an interest in examining the multiplicity of ways in which regulation is conducted in different political and cultural settings, the concept of 'risk regulation regimes' aligns well with a governmental approach to risk. Like the regime approach, an 'analytics of government' rejects totalizing assumptions about risk in contemporary life, endeavoring instead to shed light on the particular mentalities of government and administration that are brought to bear on various social problems so that they might be governed (Dean 1999). In this context, Mitchell Dean (ibid, p. 178) suggests, risk is conceived as a "calculative rationality that is tethered to assorted techniques for the regulation, management and shaping of human conduct in the service of specific ends". More precisely, an 'analytics of government' "is concerned with the means of calculation, both qualitative and quantitative, the type of governing authority or agency, the forms of knowledge, techniques and other means employed, the entity to be governed and how it is conceived, the ends sought and the outcomes and consequences" (ibid, p. 11).

Taken together, these perspectives on risk and its management offer a more differentiated view of 'risk regulation', which serves to "underscore the fact that

knowledge about risk is produced to serve different functions and under different constraints across political and cultural boundaries" (Jasanoff 1993, p. 127). Moreover, as a method of inquiry, focusing on 'risk regulation regimes' or 'regimes of government' helps mark out space "to ask questions about government, authority and power, without attempting to formulate a set of general principles by which various forms of the 'conduct of conduct' could be reformed" (Dean 1999, p. 36). In turn, this perspective offers risk scholars a means of accounting for variety across risk domains and offers insight into how various sites or regulatory activity function in practice. In particular, it sheds light on the "means, mechanisms, procedures, instruments, tactics, techniques, technologies and vocabularies" whereby "authority is constituted and rule accomplished" (ibid, p. 31), as well as the overall way risk is handled in various political and cultural settings (Hood et al. 2001).

2.5 Conclusion

As the preceding discussion underlines, there is no singular type of risk, no prescribed mode of risk measurement, and, indeed, no necessary or best response to an uncertain future event. Rather, risk-based government is plural, defined and constrained not only by the technical limitations of risk technologies, but also by the normative context within which these technologies are deployed (Fearnley 2008). The challenge, then, as a researcher, is to attend to the context-specific practices deployed in the name of managing uncertainty, without presupposing a general category of risk that pervades modern life and that limits the scope of possible responses available to society. Conceiving of risk as a 'governmental rationality' can help fulfill the former objective while helping avoid the latter. This is because this approach to risk takes as its primary site of analysis the pragmatic interventions of diverse governmental actors and organizations, and thus conceives of risk in the plural, and rejects totalizing prescriptions for change or reform (Dean 1999). An 'analytics of government', and a complimentary 'risk regulation regime' approach, in turn, not only informs risk theory, but also serves as an analytical framework for the study of risk, helping guide where one looks for data, as well as the kinds of

questions one seeks to ask of that data. In particular, an analytics of government is concerned with the 'how's' of governing, attending to the specific and not the general; informing a consistent line of questioning that is geared toward how 'regimes of practices' or 'regimes of government' operate (ibid.).

Drawing on this conceptual and analytical foundation, my thesis pursues a similar line of questioning and argumentation. That is, it endeavors to investigate the discursive and non-discursive practices presently enacted by diverse scientific and technical experts engaged in selecting, assessing and managing the risk aspects of synthetic biology in pursuit of a 'secure' and 'sustainable' science. Thus, my primary research questions ask: How is synthetic biology understood and represented as a 'biosecurity problem'? How is this problem rendered 'knowable' and 'calculable' through risk assessment techniques? What risk management strategies are proposed to mitigate these risks, and how are these justified? And, finally, what forms of 'risk responsibility' do these strategies seek to engender in synthetic biologists, and to what effect? These questions are intended to shed light, not only on the calculative techniques whereby problematic people and things are made the subjects of risk management, but also on the normative and performative dimensions of 'governing through risk' in the context of synthetic biology. In this manner, this research seeks to open up space for critical reflection on the kinds of risks synthetic biology and synthetic biologists are taken to be, how these risks are assessed and managed through risk-based techniques, and the kinds of risk responsibility these seek to engender in those engaged in various aspects of the science and its management. Before pursuing these lines of enquiry, in the following chapter I will provide a brief overview of the research process and methods used to investigate the 'risk regulation regime' examined in my thesis.

3. Methodology

3.1 Introduction

The case of 'risk management' examined in my thesis centers on a 'risk regulation regime' (Hood et al. 2001) presently orienting regulatory efforts directed at synthetic biology. More precisely, it examines how a "constellation of experts" (Rabinow 2008, p. 279) committed to advancing 'biosecurity policy'[26] – existing at the interface of 'science' and 'security' policy (McLeish and Nightingale 2007) – attempt to reconfigure seemingly 'incalculable uncertainties' as 'calculable risks' in pursuit of a 'secure' and 'sustainable' science. Informed by the work of theorists introduced in the previous chapter, the motivation for my thesis derives less from a pre-existing commitment to a particular theoretical approach or paradigm and more from a practical, albeit significant, observation made at the outset of the research process. Namely, synthetic biology has, within the last ten years, not only emerged as an exemplar of so-called 'dual-use biotechnology', but also as a site of regulatory activity characterized by the belief that even the most uncertain 'risks' (in this case, an act of 'bioterrorism') can be made the subject of practical intervention and control. In this context, an 'analytics of government' provides a suitable analytical framework for my thesis, as well as a basis for my research design.[27]

As introduced in the previous chapter, an 'analytics of government' enables researchers to approach questions about risk with a view to how 'regimes of

[26] While I will further explore (both within this chapter and elsewhere in my thesis) the nature of 'biosecurity policy', the US NIH's 'Office of Science Policy Biosecurity Program' characterizes this activity as: "the development of policies addressing life sciences research that yields information or technologies with the potential to be misused to threaten public health or national security", as well as "policies for the responsible conduct and oversight of life sciences research" (http://osp.od.nih.gov/office-biotechnology-activities/biosecurity). In this light, 'biosecurity policy' might be thought of as a form of 'science policy' or 'regulatory science' (discussed in the previous chapter) with an accent on the 'national security' aspects of modern biology.

[27] 'Research design' can broadly be defined as: 'a plan for collecting and analyzing evidence that is used to investigate and answer a specified set of research questions' (adapted from Ragin 1994, p. 191, cited in Flick 2004, p. 146).

practices' of 'regimes of government' operate, prioritizing 'how' questions (Dean 1999). Rejecting totalizing assumptions about risk, this approach does not attempt to seek answers about the 'best' way to govern, but instead to shed light on how, in practice, various governmental actors and organizations (transcending traditional notions of state rule) render disparate 'social problems' calculable and actionable through routine practices. In this context, 'risk' is conceived as a 'calculative rationality', and as a 'mode of governing', that is continually adapted and deployed to achieve specific goals. In turn, an 'analytics of government' seeks to mark out space for critical reflection about how regimes operate – characterized by specific 'techniques' and 'mentalities' of government – and, ultimately, to shed light on what is at stake in thinking and acting in a certain way (ibid.). "An analytics of government", Dean (ibid, p. 38) suggests, "removes the 'naturalness' and 'taken-for-granted' character of how things are done", thus permitting new perspectives on how things 'aught' to be and new possibilities for governing in the present.

With a view to synthetic biology, an 'analytics of government' offers a means of investigating the manner in which an emerging science is governed through an assortment of 'risk assessment techniques' and 'risk management strategies' that comprise an ongoing 'risk management process'. It also underlines the need to think critically about what sorts of 'risks' synthetic biology and synthetic biologists are taken to be, as these conceptions not only shape regulatory design, but also our collective understanding of modern biology, which is increasingly viewed through a lens of 'biosecurity'. In turn, drawing inspiration from studies in governmentality, my research methods (the subject of this chapter) describe a qualitative research project geared towards understanding the discursive and non-discursive practices enacted by scientific and technical experts (especially those in the US) engaged in various aspects of an ongoing regulatory process. Combining document analysis, semi-structured expert interviews, and observations in the field, these methods (through a process of 'triangulation', Flick 2004, pp. 178-183) were selected to offer critical insight into how governmental actors and organizations represent – and, in so doing, *construct* – a world that can be known and acted on.

3.2 My research design and the research process

The task of investigating an emerging policy debate and an ongoing regulatory process is challenging. It is challenging because the subject matter is continually evolving, with new policy proposals and revisions to existing guidelines and regulatory standards emerging (seemingly) by the day. It is also challenging because the vocabulary and definitions used to characterize 'synthetic biology' – a science that is in the process of being imagined – are in a state of flux, with each variation, evolution or revision variously characterizing synthetic biology to something 'old' – 'a continuation of genetic engineering that doesn't really require exceptional oversight and regulation' – or something 'new' – 'a technology without precedent that requires new forms of regulation and more intensive oversight'. Finally, it is challenging because 'the experts' – the 'policymakers' and 'regulators' privileged for their authoritative knowledge about the 'actual' risks, their 'implications', and 'technical' remedies – do not conform to a singular 'type'. On the contrary, they represent diverse institutions in different organizational settings, ranging from government agencies to universities, biotechnology firms to scientific advisory committees. In brief, it is challenging to analyze an emerging policy debate and an ongoing regulatory process because it is fluid and delocalized.

In light of this dynamic and distinctly heterogeneous regulatory 'space', it was evident from the outset of my research that my thesis would need to engage with a range of regulatory activities that are neither limited to a single site nor to the actions of a single overarching regulatory authority. Rather, it would need to respect that these activities are embedded in "an existing regime comprised of a collection of cooperative and coercive national and international control measures – including international agreements, multinational organisations, national and international laws, regulations, policies, norms and rules" (McLeish and Nightingale 2007, p. 1638). At the same time, it was equally evident from the outset of my research that concerns about the 'biosecurity implications' of synthetic biology (and biotechnology more generally) are especially prominent in the United States. Indeed, since the 1990s, and especially since 9/11 and the subsequent anthrax letter

attacks, US regulators have prioritized biosecurity as a core component of life science regulation (Rappert 2003; Reppy 2003; McLeish and Nightingale 2007; Collier and Lakoff 2008). It is also within the US that corresponding regulatory reforms have been the most visible, including new "biosecurity controls" on "scientific funding, peer-review, publication, employment, materials transfer, post-graduate teaching, international travel, and researchers' ability to construct, perform and disseminate research" (McLeish and Nightingale 2007, p. 1635).

With a view to these considerations, and having recently participated as an observer at the Biological Weapons Convention (BWC),[28] I was fortunate to have been granted access to the BWC as the primary site for my fieldwork. A multilateral disarmament treaty, the BWC has been described as "[t]he normative backbone" of "an existing regime" against the hostile use of modern biology (McLeish and Nightingale 2007, p. 1638) and as the "premier forum for dealing with biological threats".[29] Moreover, the BWC quite literally assembles a 'constellation of experts' (representing more than 170 countries) at Geneva's *Palais des Nations* twice a year to consider various policies, techniques and strategies for controlling the proliferation of 'dual-use' materials, technologies and knowledge relevant to the development of biological weapons. Working at the interface of the 'life sciences' and 'national security', these individuals – scientific and technical experts described by some (for example, Mukunda et al. 2009) as 'biosecurity authorities' – share a commitment to addressing the 'biosecurity risks' associated with advances in the life sciences and biotechnology. In turn, it was through my engagement with experts

[28] At an early stage of my PhD, I attended the public sessions of the August 2009 BWC Meeting of Experts and the December 2009 BWC Meeting of States Parties. In addition to observing the public sessions of these meetings, I attended related side events on synthetic biology. The first meeting included a side event on, 'The Political Implications of the Possible *De Novo* Synthesis of Smallpox' (presented by the International Security and Biopolicy Institute). The second meeting included a side event on, 'Biosecurity Risks and Assessment: Illicit Trafficking, Intangible Transfers of Knowledge, Biotechnological Advances' (presented by UNICRI).

[29] This statement was made by Ellen Tauscher, former Under Secretary for Arms Control and International Security, during an address to the Annual Meeting of the States Parties to the Biological Weapons Convention, Geneva, Switzerland, 9 December 2009, full statement available at: http://www.state.gov/t/us/133335.htm.

at the BWC, and especially with members of the US delegation (representing multiple federal departments, government agencies and affiliated institutions), that I was granted an opportunity to gain insight and proximity to a variegated regulatory space that is not easily accessible from the outside.

In addition to this fieldwork, which included a series of semi-structured expert interviews and observations at the BWC and several smaller biosecurity policy forums, my research equally drew on an extensive phase of document analysis. In particular, it drew on policy-oriented documents (see, for example, NSABB 2006; Garfinkel et al. 2007; Mukunda et al. 2009) characterizing the 'synthetic biology threat' and presenting various 'governance options' for its 'management'. In the US context, in particular, documents of this kind have proliferated in recent years, as regulatory authorities have sought guidance from scientific and technical experts perceived to possess relevant knowledge in various aspects of 'synthetic biology' and 'biosecurity'. Analyzing documents of this kind, and their 'institutionalized traces' (Wolff 2004), provided a further, rich source of data on the "institutional, governmental and discursive mechanisms" (Zinn 2004, p. 13) intended to 'steer' the synthetic biology regulatory process examined in my thesis. Taken together, this 'fieldwork' and 'deskwork' (discussed in further detail below) sought to investigate how synthetic biology is perceived to destabilize existing control measures, and how regulatory authorities and policymakers seek to overcome these obstacles in pursuit of a 'secure' and 'sustainable' science.

3.2.1 Deskwork

A technical and scientific literature review constituted the first step of the research process undertaken for my thesis. This involved, first, reading extensively on the subject of synthetic biology, and, second, examining policy-oriented documents addressing the 'dual-use' aspects of the science. In the first instance, the objective was to learn about 'synthetic biology' and 'synthetic biologists', gaining insight into how the science is described by practitioners in the field. This involved analyzing (and, in many ways, studying) articles in prominent scientific journals such as

Nature and *Nature Biotechnology*. Having an undergraduate degree in biology (specializing in animal physiology) was of some help in this regard, as I am familiar with a number of subject areas within the life sciences (for example, molecular biology, evolution and genetics), as well as a variety of associated concepts, such as metabolic pathways, genes, DNA, and so forth, discussed in the synthetic biology literature. However, as much of the language describing synthetic biology relates to new and evolving concepts such as 'biological parts', 'genetic circuits', 'synthetic genomes', and alike, much conceptual work was nonetheless required in an effort to conceive of this new way of looking at and talking about biology.

In the second instance, the objective was to survey the policy-oriented literature aimed at 'assessing' and 'managing' synthetic biology's 'biosecurity risks'. This required assembling and analyzing diverse documents, including official reports by scientific advisory committees (for example, NSABB 2006), interdisciplinary papers geared towards developing 'optimal' science policies (Garfinkel et al. 2007), and recent policy guidelines (for example, DHHS 2010b). The aim, here, was not an exhaustive mining of all available data from all available sources, but a 'theoretical sample' (Flick 2009, pp. 117-119) of the visibilities, knowledge claims, techniques and practices mobilized by experts in pursuit of representing synthetic biology as a specific kind of social problem that can be governed (Dean 1999). This process of sampling continued up to the point of encountering numerous resonances and repetitions – shared sites of interest and conflict – among comparable sources. At this time, I determined that I had reached a point of 'theoretical saturation' (Flick 2009, p. 119), which suggested that further reading would not add significant depth to the themes and conceptual categories that had already emerged from the literature. Nonetheless, from this point forward, reading was undertaken periodically, as and when scientific and technical papers were published describing new advances in synthetic biology, and the potential 'biosecurity risks' perceived to be engendered by these advances.

As a qualitative research method, document analysis (especially when combined with complimentary methods, such as qualitative interviews) offers an important tool for generating empirical data, as documents are "a means of

communication" that convey the beliefs of various social groups engaged in active processes of meaning creation (Flick 2009, p. 257). In this context, documents are not treated as static entities that convey uncontested 'facts' about the world (ibid.). Rather, they are taken to "represent a specific version of realities" that are *produced* with specific goals and audiences in mind (ibid, p. 257). In turn, "[d]ocuments can be instructive for understanding social realities in institutional contexts" (ibid, p. 262). In the case of the policy-oriented literature noted above, documents are, for example, the product of working group meetings, roundtable discussions and expert dialogues. They are the end result of a *process* of (qualitative/quantitative) assessment, interpretation, negotiation and meaning creation aimed at influencing policy design and 'steering' regulatory activities. In this light, Wolff (2004, p. 288) suggests, it is appropriate to conceive of "the nature of the document as a phenomenon". "Official documents function as institutionalized traces," enabling researchers to "draw conclusions about the activities, intentions and ideas of their creators or the organizations they represented" (ibid, p. 284).

Beyond their empirical value, the documents analyzed during this phase of the research process also helped shed light on key actors and organizations engaged in the synthetic biology biosecurity debate. This provided not only a broad sense of the policy 'network' engaged in this debate, but also helped inform my subsequent selection of "key informants" (Merkens 2004, p. 169) interviewed for my thesis. For example, it was evident at an early stage of my 'deskwork' that a small number of synthetic biologists (predominately based in the US) tend to be credited with being leaders in the field. Occupying key positions in a wider network (ibid.), these individuals are both consistent reference points for other synthetic biologists engaged in defining the 'field' of synthetic biology and for regulatory authorities concerned about synthetic biology's 'biosecurity implications'. Consequently, I recognized that interviewing one or more of synthetic biology's so-called 'key players' (de Vriend 2006) would be beneficial. Similarly, it was apparent that a number of regulatory bodies have tended to dominate the synthetic biology biosecurity debate. In the US context, for example, official reports by the National Science Advisory Board for Biosecurity (NSABB) on 'synthetic genomics' (2006),

'synthetic biology' (2010) and 'amateur biology' (2011) have been instrumental in orienting biosecurity policy discussions in the country. The product of *ad hoc* advisory committees, assembled by the NSABB and endorsed by the US government, these reports have indeed set in motion deliberative processes (often involving the formation of further technical committees recommended by the NSABB) that have provided the basis for new policy guidelines (for example, DHHS 2010b).

Based on my reading of the literature, there equally emerged consistent references to various expert 'communities' participating in the synthetic biology policy process. In particular, the notion of a 'synthetic biology community' (part of a wider 'scientific community') and a 'security community' (broadly encompassing government authorities specializing in aspects of 'national security') featured prominently in the literature. These 'communities' tended to be represented as more or less distinct social groups sharing a set of technical competencies and beliefs about the world and what might be 'best' for 'synthetic biology' (as a science) and 'biosecurity' (as a form of regulatory control). In particular, 'synthetic biologists' tended to be portrayed as 'knowing' about 'the science' (taking an interest in preserving scientific autonomy) and 'security experts' tended to be portrayed as 'knowing' about 'the security implications of the science' (favoring stronger biosecurity controls). Distinctions of this kind were especially apparent in relation to the controversial subject of censoring 'fundamental research' (discussed in Chapter 6), a subject that has raised questions about the role of national security considerations in the life sciences and the need for improved communication between science and security 'communities'. As Kwik et al. (2003, p. 32) suggest: "The idea of subjecting biological knowledge to constraints because of security concerns is a new and unwelcome notion within much of the research community." Reppy (2003, p. 45) has also pointed to tensions of this kind, suggesting that, "there is little rapport and trust between the security and biology communities", raising "important issues for the governance of science and more generally for the relationship between science and the state." In brief, while not always represented as two opposing forces, the distinction between 'science' and 'national security' –

between science and security 'communities' – was a common discursive theme in the literature and throughout the research process.

Notions of a 'scientific community' and a 'security community', while useful conceptual categories – conveying two broad professional orientations deriving from "shared expertise, norms, and worldviews" (see Davis Cross 2013, p. 157, on 'epistemic communities' and 'professionalism') – can nonetheless be somewhat misleading. Not only is this because some 'synthetic biologists' promote enhanced biosecurity[30] and some 'security experts' favor limited restrictions on scientific freedom,[31] but also because the very nature of 'biosecurity policy' is said to be both 'hybrid' and 'heterogeneous'. In the first instance, as Lakoff and Collier (2008) suggest, one of the distinguishing features of biosecurity policy is that it brings together (or blurs the boundaries between) previously distinct technical problems and political domains, notably 'public health' and 'national security'. In the second instance, biosecurity policy is said to be characterized by diverse "ecologies of experts and organizations", including "public health officials, policy experts, humanitarian activists, life scientists, multilateral agencies such as WHO, national health agencies such as the Centers of Disease Control (CDC), national security experts, physicians, veterinarians, and government officials" (ibid, p. 9).

This view of 'biosecurity policy' – as both 'hybrid' and 'heterogeneous' – was reinforced during interviews with scientific and technical experts at the BWC (discussed in the following section). Specifically, these experts frequently described themselves as having life science research backgrounds that subsequently formed the basis for their careers as 'biodefense scientists' or 'biological weapons experts'.

---

[30] For example, as Rappert (2003, p. 302) observes in relation to 'bioscience and medical communities' more broadly, bioscientists and professional organizations in the US have expressed an interest in taking greater biosecurity precautions since the 2001 anthrax attacks. Albeit, Rappert notes, the biosecurity measures put forward by these groups have primarily focused on developing "their own structures of governance before others (read: 'politicians') do for them (and do it inappropriately").

[31] For example, a consistent message (examined in further detail in Chapter 7) conveyed by the FBI to synthetic biologists and DIY-biologists is one of limiting regulatory controls on productive scientific research while maintaining a heightened sense of 'vigilance' about potential transgressions within their 'community'.

These experts equally represented a variety of professions (spread across multiple institutions), ranging from veterinary medicine to law enforcement. Thus, while science and security 'communities' are often represented as discrete social groups, underscoring different types of professional activity and varying attitudes towards 'science' and 'national security', the 'hybrid' and 'heterogeneous' nature of 'biosecurity policy' renders distinctions of this kind far more fluid than they might initially appear. Consequently, when referring to science and security 'communities' in my thesis, my intention is not to suggest that these categories are fixed and neatly bounded. Rather, it is to respect that these categories represent important discursive features of the synthetic biology biosecurity debate.

More generally, the very notion of 'experts' and 'expertise', in contrast to 'non-experts' (or 'lay-people') and 'lay-knowledge', is widely known to be problematic (see, for example, Blok et al. 2008), meriting a degree of ambivalence in forming distinctions of this kind. As Jasanoff (2003b, p. 162) suggests, "[t]oo often … experts are seen as individuals possessing special skills or superior knowledge applicable to predetermined domains of decisionmaking". In this context, the nature of expertise is 'essentialized' (Jasanoff 2003a), contributing to the belief that experts possess 'objective' knowledge that is somehow beyond the 'subjective' or 'normative' viewpoints of non-experts, and thereby necessary for formulating 'unbiased' decisions and 'appropriate' policy responses (Jasanoff 2003a; Blok et al. 2008). However, in practice, Jasanoff (2003b, p. 160) observes, "the view of the disinterested expert, standing apart from values and preferences, has all but eroded over the past few decades". In part, this more ambivalent attitude towards 'experts' and 'expertise' can be traced to the apparent 'failures' of 'expert assessments' regarding aspects of "health, safety and the environment" (ibid.), and, in part, to the substantial knowledge 'lay-people' routinely bring to bear on complex (often highly 'technical') problems encountered in their daily lives. For example, as Jasanoff (1993, p. 127) observes: "Many studies of community responses to risk have shown that citizens are capable of learning extraordinary amounts of technical information, and indeed of participating actively in creating relevant knowledge".

In this light, there is good reason to ask: who should count as an 'expert' and what should count as 'expertise' in the first place? While no one answer exists, as these distinctions ultimately rest upon subjective judgments, it is important to underline that 'expertise' is not simply an 'objective' or 'fixed' trait that exists "in the heads and hands of skilled persons, constituted through their deep familiarity with the problem in question" (Jasanoff 2003a, p. 393). In contrast, "it is something acquired, and deployed, within particular historical, political, and cultural contexts" (ibid.). Consequently, Jasanoff (2003b, p. 158) suggests, "it makes sense to look at expertise as a form of delegated authority", which, in policy contexts, lends specialists "circumscribed power" to speak for the public "on matters requiring specialized judgment." Moreover, reliance on 'experts' in policy contexts is not simply based on their capacity to generate 'objective' knowledge, but also on their capacity to 'legitimize' and 'substantiate' policy actions (Boswell 2014). In other words, "drawing on expert knowledge can be said to have a symbolic rather than a substantive value: it enhances the credibility of agencies or policy positions" (ibid, p. 7). Thus, it can be said that, "who counts as an expert (and what counts as expertise)" is contingent, responding "to specific institutional imperatives that vary within and between nation states" and over time (Jasanoff 2003a, p. 393).

Finally, as a researcher, who must also use and construct conceptual categories through which to communicate and present my argument, my own descriptions of research informants as, for example, 'synthetic biologists' or 'security professionals' (see Bigo 2000) should also be viewed as imperfect representations – as 'ideal types' – rather than 'objective' classifications. Indeed, as I have suggested, there is good reason to argue that there is no single, uniform 'science' or 'security' community to speak of. Rather, there are a 'constellation of experts' engaged in 'biosecurity policy'. In the case of those interviewed for my thesis, these designations were largely based on interviewees' self-defined professional titles, educational backgrounds, job descriptions and the national or

sub-national institutions they represented.[32] This information was used to help locate interviewees in institutional space, providing an indication of their primary professional interests and responsibilities. More broadly, my thesis draws on and tends to favor (due, in part, to the often blurred professional and epistemic boundaries of those engaged in aspects of 'biosecurity policy') the term 'scientific and technical experts' to characterize my research informants. This is to underline that these individuals, although having varying professional backgrounds, share something in common as 'first-order observers' (Luhmann 1993). That is, they view 'synthetic biology' and 'biosecurity risks' not as abstract concepts or as 'social constructs', but as first-order 'things' that can be 'known' and made the subject of practical intervention and control. In brief, 'scientific and technical experts' believe in objective 'facts' about the world and prize the accumulation of more and better information as the basis for 'rational' decision-making (ibid.).

3.2.2 Fieldwork

Drawing on the discursive themes that emerged during the course of this 'deskwork', my attention turned to conducting a series of 'semi-structured expert interviews' with scientific and technical experts engaged in various aspects of the synthetic biology biosecurity debate.[33] These interviews permitted me to further explore the discursive resonances and discontinuities identified in the literature, gaining first-hand accounts of 'synthetic biology', its potential 'biosecurity risks' and various 'policy options' for 'managing' these risks. As numerous 'qualitative interview' methods exist (Hopf 2004), it is important to underline that the choice to

[32] Each time I introduce an interviewee in my thesis, I also provide a more detailed description of their (self-defined) area(s) of expertise and institutional affiliations, for example, 'biological weapons expert working for the US Department of State'. Subsequent references to interviewees are by first and last name, often including a more concise description of their primary area of specialization, for example, 'biological weapons expert', 'public health official', or 'synthetic biologist'.

[33] In total, I interviewed 20 different scientific and technical experts. Each interview lasted approximately 1-hour. In three cases, I conducted follow-up interviews, each lasting an additional hour. See Appendix A for a list of interviewees, including brief professional profiles. See below for further details on the context of the interviews.

conduct interviews of this kind was informed by several methodological considerations and ultimately by their applicability to answering my research questions. In particular, 'expert interviews', "as a specific form of applying semi-structured interviews" (Flick 2009, p. 165), are appropriate in the case of research projects concerned with reconstructing expert knowledge, technical processes, and various institutionalized ways of thinking common to a target group (Flick 2009; Pfadenhauer 2009). In this context, what is of particular interest are the capacities of interviewees "as experts for a certain field of activity" (Flick 2009, p. 165) who often possess privileged access to information and (delegated) responsibility "for problem-solving related decisions" (Pfadenhauer 2009, p. 83).[34]

Recognizing that being granted access to interview subjects is difficult, especially when 'interviewing up', this fieldwork was greatly aided by the contacts that I had recently established as an observer at the biannual meetings of the BWC, as well as at several other workshops and conferences related to synthetic biology and its perceived 'biosecurity implications'.[35] Having a background in biology and a familiarity with the subjects of 'synthetic biology' and 'biosecurity' (due, in part, to the earlier scientific and technical literature review, and, in part, to my experiences at the biosecurity forums noted above) was equally advantageous. In particular, this enabled me to (at least in part) "'speak the same language'" (Heyl 2001, p. 371) as the interview subjects consulted for my research. In the case of expert interviews, in particular, demonstrating a level of "thematic competence" (Pfadenhauer 2009, p. 90) in the subject matter under investigation is said to be essential for asking the right questions" and "probing in an appropriate way" (Flick 2009, p. 168). In essence, expert interviews are said to require that the interviewer take on the role of 'quasi-expert' in an effort to break down communication barriers, build trust, more easily establish a good rapport, and (to the extent possible) "conduct a conversation 'on equal footing'" (Pfadenhauer 2009, p. 91).

---

[34] This can be contrasted with, for example, 'biographical interviews', which are primarily concerned with interviewees' individual life histories (Flick 2009).

[35] These workshops and conferences will be discussed in further detail below.

Balancing the time required to conduct and transcribe my interviews (23 in total, each lasting approximately 1-hour) against the need to ensure the 'quality' of the collected data (Merkens 2004), my selection of interviewees focused on 'good informants' (Flick 2009). Although multiple criteria exist for identifying 'good informants', at minimum these individuals should possess practical (or 'operational') knowledge and proximity to the research subject under investigation and be willing to participate in the study (Flick 2009; Pfadenhauer 2009). Moreover, the selection of interviewees, like other sources of empirical data, should represent "the case [under investigation] with as many facets as possible" (Merkens 2004, p. 167). With a view to these considerations, and in light of the many types of scientific and technical experts represented in the literature; the diverse composition of experts represented at the BWC, and based on several exploratory talks with experts prior to my fieldwork, it was apparent that my interviews would need to include a relatively wide range of professionals engaged in 'biosecurity policy'.

Focusing primarily on experts working in the US context, my interviews were conducted in person at two, weeklong meetings of the BWC in Geneva (23-27 August 2010; 6-10 December 2010), in addition to several interviews at the LSE's BIOS Centre and over Skype. These interviews were conducted with: leading synthetic biologists who have been instrumental in defining the 'field' of synthetic biology; law enforcement agents responsible for 'biosecurity awareness raising' activities with synthetic biologists and 'do-it-yourself (DIY) biologists'; public health officials overseeing 'community labs' engaged in 'DIY-biology', and disarmament experts conducting 'biosecurity outreach' activities at the annual International Genetically Engineered Machine's (iGEM) competition. Interviews were recorded and later transcribed and coded (see Flick 2009, pp. 305-332, on "Coding and Categorizing") with a view to the conceptual categories and themes identified during the earlier literature review, as well as further 'discursive patterns' (Coyle 2007) visible in the interview texts. With the exception of several interviews conducted with military biodefense scientists, interviewees permitted me to use their real names. In accordance with the sensitivity of some of the information that

was shared with me, as well as the LSE's Research Ethics Policy,[36] interviewees were informed of how I would use their interview data and offered the opportunity to review the interview transcripts in advance of this data being used.[37]

Finally, my research also drew on informal discussions and observations made at the BWC and during several other workshops and conferences, including: the Geneva Forum's workshop series on, 'Enhancing the BWC Confidence Building Measure Regime' (Jongny, 22-23 August 2009; Geneva, 12 December 2009; Berlin, 26-27 April 2010); the United Nations Interregional Crime and Justice Research Institute's (UNICRI) 'Synthetic Biology and Nano-biotechnology Risk and Response Assessment Project' (Turin, 24-25 March 2010 and Geneva, 16-17 June 2010), and Cesagen's workshop entitled, 'Microbiology, genomics, and beyond: Regulating dual use technologies in the 21st Century' (London, 17 September 2010). While each of these meetings focused on synthetic biology (as the primary topic of discussion) to varying degrees, several overarching themes emerged that were particularly relevant to understanding the nature of the synthetic biology biosecurity debate examined in my thesis. First, experts at each of these meetings tended to present synthetic biology as posing 'unique biosecurity challenges', which were believed to require 'existing regulatory structures' to be 'reconsidered or revised'. At the same time, it was equally apparent that many of the same experts believed that it is 'possible', if not 'necessary', to 'encourage scientific progress' and 'minimize the risk of deliberate misuse'. In this light, 'the challenge facing regulators' tended to be framed as one of finding 'appropriate regulatory strategies' to achieve this objective. Lastly, it was often suggested that any effort to 'regulate' or 'manage' synthetic biology's 'biosecurity risks' would depend upon the capacities of scientific and security 'communities' to 'work together' towards this 'shared goal'.

Although my role as a 'participant observer' (Atkinson and Hammersley 1994) at these events was limited in scope,[38] this fieldwork nonetheless offered a

[36] This included completing the 'LSE Research Ethics Review Checklist', available at: http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/resEthResChe.pdf.
[37] Ultimately, few interviewees opted to redact or modify the interview transcripts. Those modifications that were made largely involved clarifications (for example, adding detail to a specific response) rather than substantive changes.

valuable 'snapshot' of the social phenomenon under investigation (Flick 2009). In particular, unlike the more structured interview environment, observations collected (transcribed as field notes and later categorized and coded) at these meetings enabled me to observe how, in a more 'natural' setting (ibid.), scientific and technical experts talk about synthetic biology as a specific kind of 'social problem'; the forms of reasoning and types of certified knowledge brought to bear on this problem, and the methods of negotiation and compromise deployed in determining 'appropriate policy solutions'. In addition, this level of proximity to biosecurity policy discussions offered the possibility of relatively subtle observations, which often drew as much on visual cues, the tone of a participant's voice, or the personal opinions participants shared with me during breaks in the meetings, as they did formal statements. This revealed, for example, that despite frequent claims of 'working together', 'life scientists' and 'security experts' (when these two 'communities' can be differentiated) often display different attitudes towards the role and importance of 'national security' considerations in the life sciences, suggesting (at times) a far more 'uneasy' partnership between 'scientists' and 'security experts' than might otherwise be communicated.

Through this research process, which combined document analysis, qualitative interviews and observations in the field, I gained a broad sense of the structure and composition of the 'policy constellation' that comprises the synthetic biology biosecurity debate examined in my thesis, as well as gaining insight into the discursive themes and conceptual categories that characterize this debate. Moreover, by opting to use several methods, each geared towards understanding the discursive and non-discursive practices deployed by experts engaged in aspects

[38] In contrast to ethnographic studies, which tend to involve the researcher becoming immersed in a social group over an extended period of time, my 'participation' at these meetings was limited. In fact, to the extent possible, I sought to maintain a degree of 'distance' (Flick 2009) from the subject matter being discussed in an effort to not overly influence the events observed at these meetings. Yet, as all forms of social research are arguably a form of 'participant observation', in as much as a researcher "cannot study the social world without being part of it" (Atkinson and Hammersley 1994, p. 249), it remains appropriate to describe my role as that of a 'participant observer'.

of 'biosecurity policy', I endeavored to limit the interpretive bias of my results and to maximize their generalizability. As Flick (2009, pp. 26-27) suggests, combining complimentary methods ('triangulation'), integrated into a coherent research design, can help compensate for "the weakness and blind spots of any single method", offering a more accurate representation of the social world. At the same time, no matter how well conceived the research design, it is important to acknowledge that the research process is never 'neutral' or 'apolitical', but rather it is the outcome of numerous choices, which place constraints upon the 'scope' and 'quality' of the research (ibid.). In turn, it is necessary to consider my own role in the research process, and the potential limitations of my research design.

3.3 My role in the research process and the potential limitations of my research design

That knowledge about the world is not simply a "portrayal of given facts, but [the outcome of] a process of active production" is a central tenant of social constructivism and a cornerstone of much qualitative research (Flick 2009, p. 70). Indeed, the belief that 'facts' do not simply exist 'out there', beyond the social world, but are produced through social interactions, can be said to provide much of the motive force behind critical research in the social sciences. In turn, to adopt this perspective, as a researcher, one must equally acknowledge one's own role in the research process, which is no less an 'active process of (re)construction' (Flick 2009; Denzin 2004). As Denzin (2004, p. 86) observes: "There is no mirror of nature" and, thus, no 'singular' or 'objective' mode of enquiry. Rather, "the world as it is known [by social scientists or anyone else] is constructed through acts of representation and interpretation" (ibid.). In this light, far from being a passive observer of 'facts' about the social world, the researcher can be seen to play an integral role in all aspects of the research process (Lincoln 2004), including the selective work of choosing 'social groups' or 'cases' of interest to the research (Merkens 2004, p. 167); the documentary materials and interview subjects; the collection and interpretation of data, and, ultimately, the manner in which this data is organized and presented. In

brief, at all phases of the research process, numerous choices must be made, which both define and constrain the 'scope' and 'quality' of a research project.

In the case of my thesis, several considerations can be said to have shaped the 'scope' and 'quality' of my research. In the first instance, it is important to acknowledge that the overall focus (and, in turn, the *scope*) of my thesis sheds light on certain aspects of the 'social and ethical debate' on synthetic biology, while obfuscating others. In particular, my thesis engages with only one aspect of this debate, namely the 'biosecurity implications' of synthetic biology and the various 'risk assessment techniques' and 'risk management strategies' that have, in recent years, been brought to bear on this highly specific policy 'problem' with a view to finding practical policy 'solutions'. Moreover, in choosing to focus on 'scientific and technical experts' (particularly those working in the US context) engaged in aspects of 'biosecurity policy', I have, to some extent, excluded other social groups (who no less have a stake in determining the acceptability and future direction of synthetic biology) from this discussion. For example, my thesis does not take as its focus 'risk perception' among members of the so-called 'lay-public'.[39] Thus, in choosing to focus on a specific segment of a much wider social phenomenon, it is important to acknowledge that my thesis cannot (nor does it claim to) provide a comprehensive picture of 'the' social and ethical debate on synthetic biology.

In the second instance, it is equally important to consider how choices made at subsequent stages of the research process could have influenced the *quality* of my research. For example, in addition to choosing to focus on a specific aspect of a wider social and ethical debate on synthetic biology, my research also depended upon choices regarding the selection of interview subjects who 'represent' the case of interest. These choices, although informed by my literature review and my

[39] Yet, nor should this decision be seen as arbitrary. As I have suggested, the 'policy constellation' engaged in 'biosecurity' consists primarily of experts with 'operational' knowledge in various aspects of 'public health', the 'life sciences' and 'national security'. Therefore, it is arguably appropriate that my thesis focuses on these groups of actors. Moreover, at present, at least in relation to the 'lay-public', it should be noted that there exists limited 'public awareness' of 'synthetic biology', thus limiting the possibilities for empirical research on 'public risk perception' of the field.

experiences at various biosecurity policy forums (as I have noted), inevitably excluded some actors who certainty possess 'practical knowledge' on aspects of 'synthetic biology' and 'biosecurity'. Moreover, the interview experience itself is shaped by numerous choices, as well as a range of contingencies that result from reciprocal interactions between interviewer and interviewee. According to Hermanns (2004), these factors contribute to shaping the 'interview drama', and the resulting 'co-produced' knowledge. In this light, although I prepared an 'interview guide' to help orient my interviews towards a series of 'open' questions designed to help answer my research questions (Hopf 2004), additional factors, including the choice of interview environment and the quality of my own 'performance' as an interviewer (Hermanns 2004; Hopf 2004), inevitably influenced the direction interviews took, and the content of the interview data. Lastly, it is important to underline that my interpretation and presentation of the data – an exercise that depends upon forming conceptual categories, defining discursive themes and grouping multiple strands of information together to produce a generalizable 'picture' of the social world – was itself a 'process of (re)construction', requiring numerous choices to be made. Thus, even though my analysis was informed by an 'analytics of government', which "singles out for special attention … the practices and forms of reasoning that shape technical response" (Collier et al. 2004, pp. 6-7), multiple interpretations of the same data are always possible.

Finally, in addition to these considerations, and the possible empirical constraints and limitations they may place on my research, there is an 'ethical' dimension or 'dilemma' to my research that I feel warrants acknowledgment. That is, like the diverse scientific and technical experts with whom my thesis engages, who discuss the 'synthetic biology threat' and possible ways of 'assessing' and 'managing' this 'threat', my own contribution to this debate, albeit from the critical standpoint of a 'second-order observer', to some extent contributes to reifying anxieties about future events that may never happen. Thus, I would like to acknowledge that I take responsibility for my own performance in this debate, and recognize that talking about issues such as 'bioterrorism' and 'biological weapons' is never unproblematic, no matter how 'critical' my perspective may be. Yet, like

Rappert (2003, p. 303), I also recognize that "the topic of biological weapons has received scant [albeit growing] attention in the past in many social science fields", making the need for critical research in this area all the more important. Thus, despite the dilemma faced by those engaged in this line of research, it should not, in my opinion, discourage scholarly discussion and debate. Rather, I believe it is important to discuss these issues openly, and through this discussion contribute to changing the tenor of the debate for the better; and this by way of bringing to the surface some of the taken-for-granted assumptions and unquestioned categories that might otherwise be less likely to emerge and be critically discussed.

3.4 Conclusion

In this chapter, I have endeavored to provide a rationale for my research design and outline the research process undertaken to answer my research questions. In the first instance, I have argued that an 'analytics of government' provides a suitable analytical framework for my thesis, as well as a basis for my research design, in as much as this approach to risk pursues a consistent line of questioning geared towards understanding how 'regimes of government' or 'regimes of practices' operate (Dean 1999). In the second instance, I have described the research process I have undertaken, including my identification of the social group (a 'constellation of experts' engaged in 'biosecurity policy') of primary interest to my thesis and the 'qualitative research methods' (including document analysis, expert interviews and observations in the field) selected to shed light on the discursive and non-discursive practices that comprise the synthetic biology biosecurity debate. Finally, I have endeavored to consider my own role in the research process, underlining how my choices have played an integral role in determining the 'scope' and 'quality' of my research. Taken together, this chapter describes a qualitative research project that has been designed to understand how scientific and technical experts engaged in biosecurity policy render a seemingly 'incalculable risk' 'knowable' and 'actionable' in pursuit of a 'secure' and 'sustainable' science. My thesis, in turn, attempts render

this activity – one aspect of the social world – visible with a view to understanding how, and to what effect, synthetic biology is 'governed through risk'.

4. Risk selection: Constructing a 'taxonomy of difference'

4.1 Introduction

Amidst growing concerns about synthetic biology's potential 'biosecurity risks', it is rarely acknowledged that to speak of synthetic biology in relation to 'biosecurity' is already a highly specific framing of a 'problem' to be 'solved'. There are, after all, any number of ways in which synthetic biology might be framed as problematic, each presupposing particular kinds of worries, dilemmas, and possible future harms. So why do many scientific and technical experts engaged in aspects of the ongoing synthetic biology policy debate privilege this particular problem (or set of problems)? What is it about synthetic biology and its diverse practitioners that is perceived to be 'dangerous' or 'of concern'? And how do these 'concerns' orient risk management efforts and delimit the possibilities for regulatory intervention and control? These are just some of the reflexive considerations, I suggest, that need to be brought to the surface in an effort to understand what is at stake in framing synthetic biology as a specific kind of problem for risk management.

With a view to these research questions, in this chapter I will examine the selective processes experts employ in their efforts to define and demarcate the boundaries of what is 'dangerous' or 'of concern' in synthetic biology. My argument is developed in several sections. First, I underline that, in the United States (US), in particular, the material and informational elements that makeup modern biology are increasingly framed in relation to the threat of 'bioterrorism' and in accordance with the norms and logics of 'biosecurity' – a defensive practice premised upon keeping 'dangerous tools' out of 'dangerous hands'. Second, I situate synthetic biology in this context, examining how it is perceived to complicate the goals of biosecurity by way of enabling more people to gain access to 'potentially dangerous' biological materials and information (an expectation that builds on synthetic biologists' own claims about the potential of their science to 'democratize' modern biology). Finally, I conclude by way of reflecting on the manner in which scientific

and technical experts draw on notions of 'difference' or 'otherness' – a 'different way of doing biology' and a 'different way of being a biologist' – to not only describe but also produce a new set of 'problems' and 'risks' to be assessed and managed.

This research suggests that, for many scientific and technical experts, synthetic biology is perceived to be problematic because it disrupts existing approaches to biosecurity. In effect, synthetic biology is undergoing a process of 'problematization': that is, it has been interpreted as destabilizing conventional ways of knowing and understanding the world, motivating a regulatory response that seeks to reestablish continuity and order in the face of uncertainty and change. In this light, 'risk selection' – whereby risks are identified, classified and given a name – can be understood as the process of surfacing those aspects of synthetic biology that do not conform to the prevailing logics of biosecurity, setting them apart as 'risk objects' of regulatory interest and concern. Resembling taxonomy – a practice that depends upon classifying and naming a set of elemental parts that can be (re)configured according to specific rules – risk selection is both descriptive and inventive, drawing on experts' capacities to identify and produce new 'kinds' of people and things to be governed through risk management.

4.2 Framing the threat

In this section, I will introduce several interrelated subjects and concepts that help shed light on why synthetic biology is perceived to pose 'biosecurity risks' in the first place. In particular, I underline that, in recent years, 'bioterrorism' has emerged as a key subject of regulatory interest and concern within life science policy circles, especially in the US. Moreover, although there have been few historical instances of bioterrorism, and expert opinion varies as to the 'likelihood' and 'consequences' of this type of event, 'concerns about bioterrorism' have had a significant impact on the life science regulatory environment. Next, I take a closer look at the concept of 'biosecurity', which, for the scientific and technical experts consulted for my research, represents a technical 'solution' to the 'problem' of bioterrorism. Finally, I consider how, in this context, synthetic biology is perceived to be especially

problematic. Specifically, synthetic biology is perceived to complicate, if not undermine, the norms and logics of biosecurity – a defensive practice borne out of growing concerns about bioterrorism and premised upon keeping 'dangerous tools' out of 'dangerous hands'. In this light, much of what is perceived to be problematic about synthetic biology in relation to its 'regulation', which I will explore in depth during the remainder of the chapter, can be traced to this highly specific framing of 'risk' and 'risk management' in the contemporary life sciences.

4.2.1 Focusing on bioterrorism

Although there have been few historical instances of 'bioterrorism',[40] and none that have approached the 'worst-case scenarios' predicted by some, 'concerns about bioterrorism' are real enough. Indeed, since the mid-1990s, largely in response to a perceived link between international terrorism and the possible use of biological weapons in a terrorist attack, many policymakers, especially in the US context,[41] have come to view bioterrorism as a 'catastrophic' threat (Wright 2004). Compounding these concerns, in the aftermath of the events of 9/11 and the subsequent anthrax letter mailings, it is all but taken-for-granted in US policy circles that there exists an urgent and legitimate need to prepare (and to be seen to prepare) for this contingency (Rappert 2003; Reppy 2003; Wright 2004). In a recent report presented to the US Congress, for example, the science and technology policy

[40] According to arms control scientist Milton Leitenberg's (2005, p. 22) analysis of five extensive databases covering all known bioterrorism-related "events" in the twentieth century, there have, in fact, been only four instances involving "the preparation or attempted preparation of pathogens in a private laboratory by a nonstate actor." These include the Rajneesh's deliberate contamination of salad bars using salmonella in 1984 in Oregon, which resulted in 750 cases of food poisoning; the Aum Shinrikyo cult's "unsuccessful attempts to procure, produce and disperse anthrax and botulinum toxin" between 1990 and 1994 in Japan; Al-Quaeda's unsuccessful attempts to procure anthrax and establish a functional biological weapons laboratory in the late 1990s in Afghanistan; and "the successful 'Amerithrax' distribution of a high-quality dry-powder preparation of anthrax spores" in the US in 2001, which resulted in five deaths.

[41] While heightened concerns about bioterrorism and the subsequent addition of new 'biosecurity controls' have been the most evident in the US, the UK (among other countries) has also seen an increased focus (albeit to a lesser degree) on bioterrorism and biosecurity in recent years (see, for example, McLeish and Nightingale 2005).

specialists Gottron and Shea (2011, p. 4, emphasis added) observe that, although bioterrorism has been a topic of concern for US policymakers for sometime, these more recent events have "led to an *increased focus* on terrorism in general and especially on biological weapons of mass destruction (WMDs)." As Rappert (2003, p. 99) has similarly argued, these events "served as a punctuating point", motivating not only regulatory authorities but also life scientists and professional organizations to consider various measures aimed at countering the threat of bioterrorism (in part, as a preemptive measure against 'reactionary' government legislation).

Hand-in-hand with an increased focus on bioterrorism, there has also been an increased focus on 'non-state actors'. The origin of these concerns is often traced to the collapse of the former Soviet Union, which is said to have elevated (particularly in the US context) the perceived threat that individuals, as opposed to states, could exploit modern biology for destructive purposes. Central to these accounts, as Collier et al. (2004, p. 6) note, are concerns about former Soviet scientists "with weapons-relevant expertise" who "have 'melted away' and are unaccounted for" following the dissolution of the Soviet Union and its accompanying weapons programs. Adding to these concerns, McLeish and Nightingale (2007, p. 1640) suggest, the growing accessibility of biological materials, laboratory equipment and advanced life science knowledge (all of which have 'legitimate' research applications) is often cited as enabling individuals to circumvent the financial costs and technical barriers associated with biological weapons development. In turn, in contrast to a former era characterized by the perceived threat of state-level 'biowarfare', individuals (including life scientists, who are perceived to have privileged access to potentially dangerous life science resources) are increasingly viewed "as both sources of threat and as sources of technological capabilities" (ibid.). As McLeish and Nightingale suggest (ibid.), this "marks a new development in biosecurity policy, which historically has been state-centric because only states were able to afford to development biological weapons."

At the level of life science regulation, the growing emphasis on non-state actors has also contributed to a decline in the perceived relevance of control efforts "based on bilateral or multilateral agreements among states" and the ascension of

"new strategies for regulating biological warfare knowledge" (Collier et al. 2004, p. 6). Specifically, as McLeish and Nightingale (2007, p. 1640) suggest, a new "regime has evolved" that places a greater emphasis on the part of national governments on regulating the conduct of life scientists, encompassing "new controls on people, experiments and the flow of information, technology and materials."[42] Circumscribed under the heading of 'biosecurity policy', "[t]hese national controls are now the main vehicles that govern scientific activity" (ibid). At the same time, individuals who are "not normally associated with security" have been enrolled in combating the perceived threat of bioterrorism (ibid.). In particular, life scientists are increasingly conceived as 'guardians of science' – actors who are essential to monitoring and preventing the 'deliberate misuse' of modern biology, including potential transgressions within their 'community'. Taken together, these new regulatory measures, whether voluntary or enforced, implemented at the level of national governments or sub-national institutions, comprise an evolving 'governance system' comprised "of international agreements, legal regulations, professional standards, ethical mores, and catalogues of 'best practices'" intended to ensure sustainable progress in the life sciences (Kwik et al. 2003, p. 27).

While concerns about bioterrorism have grown in prominence in recent years, having important consequences for life science regulation, expert opinion nonetheless varies as to the 'likelihood' and 'consequences' (the standard metrics of 'quantitative risk assessment') of these sorts of events. In part, as I have suggested, this is because there have been few historical instances of bioterrorism, and, in part, because there exist very different opinions about the technical feasibility of producing viable biological weapons. With a view to the second source of uncertainty, some describe bioterrorism as the 'poor man's atomic bomb',[43]

[42] It is important to note, as McLeish and Nightingale (2007, p. 1648) underline, that: "While the most extensive controls have been introduced in the USA, the extent of international collaboration with the US science system, the adoption of similar measures by the EU, and the importance of global implementation for their effectiveness, suggests that these controls will diffuse for the foreseeable future".

[43] Characteristic of this view, Jeremy Rifkin (2001) underlines that biological weapons (including "genetic weaponry") can justifiably be described as the 'poor man's atomic

underlining the belief that it is relatively affordable and easy to produce biological weapons, and, moreover, that their use could have 'catastrophic' consequences.[44] From the perspective of these commentators, it is not so much a question of 'whether' a large-scale act of bioterrorism will happen, but rather 'when' it will happen.[45] On the other hand, just as many experts suggest that it is relatively difficult to produce biological weapons, not only due to the challenges associated with acquiring dangerous pathogens (for example, smallpox), but also due to the 'downstream' technical difficulties associated with transforming pathogens into viable weapons. A multi-step process, 'weaponizing' pathogens is said to require producing a sufficient quantity of pathogenic material, which can be stored, transformed into an environmentally stable product, and successfully disseminated over a large area to cause 'mass casualties' (Leitenberg 2005). From the perspective of this second group of commentators, the paucity of historical data on bioterrorism is therefore not so much a reflection of a lack of intent on the part of individuals, but a consequence of the technical challenges confronting individuals or terrorist groups who might wish to produce a true 'weapon of mass destruction'.

The question of whether bioterrorism represents a 'viable' and potentially 'catastrophic' threat or whether the threat is overstated due technical challenges associated with 'weaponizing' pathogens remains an ongoing source of debate among experts. Moreover, contrasting opinions exist between countries as closely allied as the United States and the United Kingdom (see Rappert 2003), with the US, as I have said, placing considerably more emphasis on bioterrorism within their national 'portfolio' of biological 'risks' and 'threats'. Yet, irrespective of the 'actual' risks – their 'likelihood' and 'consequences' – 'concerns about bioterrorism' have

---

bomb' as they could pose "a similar threat to our very existence", and, "unlike nuclear bombs, the materials and tools required to create biological warfare agents are accessible and inexpensive" (http://articles.baltimoresun.com/2001-10-07/topic/0110050346_1_biological-warfare-biological-agents-biological-weapons).

[44] See, for example, *The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats*, Vol. I, Final Report, October 1997.

[45] Leitenberg (2005, p. 105) notes that: "The two main popularizers of this phrase, in innumerable press, radio and TV interviews, were Drs. D.A. Henderson and Michael Osterholm" (vocal contributors to the 'bioterrorism-catastrophic-potential' discourse).

had a significant impact on the manner in which modern biology is understood, represented, and made the subject of regulatory intervention and control. Indeed, as multiple scholars (Rappert 2003; Reppy 2003; McLeish and Nightingale 2007, among others) have pointed out, concerns about bioterrorism have contributed to increased spending on national 'biodefense' programs; an increased accent on preventing the 'deliberate misuse' of modern biology; the design and implementation of new national legislation; the promotion of 'self-governance' mechanisms, and the development of new oversight and regulatory strategies aimed at monitoring and controlling flows of materials and information relevant to the production of biological weapons. In brief, as the science and technology scholar Judith Reppy (2003) rightly argues, concerns about bioterrorism have "changed the political and social context for biological research" (ibid, p. 40) and contributed to a "permanent shift" in the research and regulatory environment, "the full consequences of which are still to be revealed" (ibid, p. 49).

4.2.2 The 'dual-use dilemma'

In light of growing concerns about bioterrorism, advances in the life sciences are increasingly characterized as possessing an innate 'dual-use potential'. That is, the necessary 'ingredients' for doing biology are perceived to enable, on the one hand, 'revolutionary' advances in health, medicine and industry, and, on the other, new threats to 'public health' and 'national security' (Kwik et al. 2003). Popularized by the so-called 'Fink Committee', in a report published by the US National Research Council (NRC) in 2004,[46] this characterization of modern biology is inscribed under the concept of the 'dual-use dilemma'. In the words of the Fink Committee, an *ad hoc*

[46] The Fink Committee, otherwise known as the 'Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology', was composed predominantly of life scientists, guided by the contributions of a select number of security advisors and biological weapons experts. One member of the Fink Committee, David Franz (introduced in further detail below), was interviewed for my research in the context of the Biological Weapons Convention (BWC).

advisory committee named in honor of the Committee's chair, Gerald Fink, a genetics professor at the Massachusetts Institute of Technology (MIT):

> "The great achievements of molecular biology and genetics over the last 50 years have produced advances in agriculture and industrial processes and have revolutionized the practice of medicine. The very technologies that fueled these benefits to society, however, pose a potential risk as well – the possibility that these technologies could also be used to create the next generation of biological weapons. Biotechnology represents a 'dual use' dilemma in which the same technologies can be used legitimately for human betterment and misused for bioterrorism." (NRC 2004, p. 1)

The 'dual-use dilemma', as a concept that has been widely adopted by scientists, security experts, public officials, and many others, has in effect 'unlocked' a new set of possibilities for biotechnology, directing attention towards a new set of 'problems' and 'potential risks'. More than ever before, advances in biotechnology are accompanied by an expectation of 'deliberate misuse' and the possibility of 'catastrophic harm'. Moreover, concerns of this kind are increasingly located in the material and informational elements that makeup modern biology, which are represented as possessing 'fixed' functions that are 'intrinsically dangerous' (McLeish and Nightingale 2007). Indeed, the Fink Committee's primary aim, and one that has been taken up and advanced by diverse bureaus, departments, agencies, *ad hoc* committees and working groups, both in the US and elsewhere, was to explore and to categorize, "the capacity for advanced biological research activities to cause disruption or harm, potentially on a catastrophic scale" (NRC 2004, p. 1).

Conceptually, the 'dual-use dilemma' can be thought of as enabling the production of new 'risk objects' – "ideas about harm with implicit causality" – that can be made the subject of risk management or regulation (Power 2007, p. 25). Indeed, a further legacy of the Fink Committee was their introduction of seven categories of problematic experiments – labeled 'experiments of concern' (NRC 2004) – that the Committee argued could enable the production of (enhanced) biological weapons. This new emphasis on 'dual-use research' has, in turn, had the effect of expanding the scope of life science oversight and regulation, which is now

focused not only on pathogens and advanced technologies, but also on life science knowledge, including its production and dissemination. In this manner, to an existing list of high-risk pathogens (known, in the US context, as 'Select Agents')[47] and an array of modern laboratory equipment, there exist growing concerns about genetic information, research activities, scientific protocols, and alike. Moreover, according to the Fink Committee, this catalogue of risks is far from complete:

> "The great diversity as well as the pace of change makes it imprudent to project the potentialities both for good and ill too broadly and too far into the future. Therefore, the Committee has initially limited its concerns to cover those possibilities that represent a plausible danger and has tried to avoid improbable scenarios. Over time, however, the Committee believes it will be necessary to expand the experiments of concern to cover a significantly wider range of potential threats." (NRC 2004, p. 6)

In brief, under the "the ever-elusive category of 'dual-use research'", as the anthropologist Carlo Caduff (2008, p. 272) has rightly argued, "the potential scope of regulatory intervention is in fact infinitely expandable."

4.2.3 'Guns, gates and guards': Introducing the 'classical' biosecurity model

In tandem with the production of new 'risk objects', which have been defined on the basis of the 'dual-use dilemma', there has been an appreciable shift in the US regulatory environment from a regulatory focus on 'biosafety' to 'biosecurity' (Reppy 2003; Atlas 2005b). As McLeish and Nightingale (2007) suggest, this shift has been accompanied by "new governance measures" (ibid, p. 1643) "that focus on restricting the diffusion of dangerous scientific information, pathogens and materials" (ibid, p. 1644). Characteristic of these reforms, the US Patriot Act (2001)[48] and US Public Health Security and Bioterrorism Preparedness and Response Act (2002),[49] legislation introduced following the terrorist attacks of

[47] See http://www.selectagents.gov/.
[48] See http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.
[49] See http://www.gpo.gov/fdsys/pkg/PLAW-107publ188/pdf/PLAW-107publ188.pdf.

2001, imposed new control measures on "select agents (i.e., those pathogens considered likely to be used in biological weapons)", including mandatory registration requirements for laboratories handling Select Agents, FBI background checks on researchers working with Select Agents, and rules forbidding 'restricted persons'[50] from gaining access to Select Agents (Reppy 2003, p. 38). Although only one component of a wider regime aimed at countering the threat of bioterrorism, these reforms are illustrative of a distinctive functionality and set of underlying logics characteristic of biosecurity. In particular, they underline how biosecurity (as the concept is understood in the US regulatory context) is conceived as a specific kind of technical 'fix' to the 'problem' of bioterrorism. The nature of biosecurity can be further clarified when it is compared with the well-established practice of biosafety. Although both biosafety and biosecurity broadly describe a mechanism of control, they are each directed at managing two very different kinds of 'risk'.[51]

In the case of biosafety, which prior to 2001 had been the primary focus of life science regulatory strategies in the US (Reppy 2003; Atlas 2005a), risk management efforts are directed at controlling the 'unintended consequences' of life science research. This framing, which was influenced by scientific and technical deliberations on recombinant DNA technology in the 1970s (Wright 1986), locates 'risk' in the laboratory, embodied in the hazardous materials handled by life scientists (Caduff 2008). The accompanying risk management strategies are based on a principal of containment (ibid.), whereby experiments and experimental products are kept within the confines of controlled research settings, exemplified by "rules governing laboratory design and research practices intended to protect workers and the general public from inadvertent release of biopathogens or potentially dangerous genetically engineered agents" (Reppy 2003, p. 40). 'Biosafety

[50] According to the US Patriot Act (2001, section 175b), 'restricted persons' include, among others, convicted criminals (incarcerated for more than one year), fugitives, unlawful users of controlled substances, the mentally ill, and illegal aliens (http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf).

[51] See 'Biosafety and Biosecurity', an explanatory document prepared by the BWC Implementation Support Unit, available at: http://www.unog.ch/80256EDD006B8954/(httpAssets)/46BE0B4ACED5F0E0C125747B004F447E/$file/biosafety%2Bbackground%2Bpaper%2B-%2Badvanced%2Bcopy.pdf.

risks', in turn, are typically understood and represented as the unintended byproduct of experimental error or scientific negligence, and the primary responsibility for risk management falls upon scientists who are intended to monitor their own conduct in an effort to minimize unintended harm.

Biosecurity, in contrast, broadly describes a set of practices directed at preventing the 'deliberate misuse' of modern biology by sub-state groups or individuals, calling for sustained 'vigilance' on the part of scientists (as well as biotech companies, scientific publishers, and others) to guard against potential transgressions within their 'community'. In other words, it is intended to confront and control the perceived threat of bioterrorism. In practice, even though definitions of 'biosecurity' vary between countries and 'biosecurity controls' are continually evolving in tandem with the emergence of new 'dual-use concerns', for US authorities engaged in aspects of 'biosecurity policy', biosecurity is typically defined by a finite set of characteristics, which set it apart from biosafety and other modes of managing biological risks (for example, public health). According to the US National Science Advisory Committee for Biosecurity (NSABB 2010, p. 10), to offer a general overview, biosecurity "refers to the protection, control of, and accountability for high consequence biological agents and toxins, and critical relevant biological materials and information," and preventing "unauthorized possession, loss, theft, misuse, diversion, or intentional release."

Interviews conducted with several biological weapons experts in the context of the Biological Weapons Convention (BWC) further capture much of what is distinctive about biosecurity, as a particular kind of technical 'fix' to the problem of bioterrorism. For Dana Perkins, a public health official and biological weapons expert working for the US Department of Health and Human Services (DHHS):[52]

> "[B]iosecurity, nowadays, means physical security of biological agents. Basically we have a list of agents and we know we have to keep them under lock and key; scrutinize the people that work with those agents; and control

[52] Please note: Dana Perkins now works for the United Nations Security Council 1540 Committee. However, throughout my thesis, I refer only to Perkins' professional responsibilities at the time of our interview.

> information related to the facilities they're in; their transportation; their genetic information, and so on." (Dana Perkins)

In other words, biosecurity is said to involve controlling access to potentially dangerous biological materials and information – most notably, biological materials and information related to 'Select Agents' (a list of microorganisms and toxins that are believed to be especially suitable for use as biological weapons).[53]

Other biological weapons experts interviewed in the context of the BWC described biosecurity as, "locking up bugs" (Piers Millett) or "prevent[ing] bugs from theft or diversion" (Richard Weller). From this perspective, the source of concern is more narrowly conceived as pathogens ('bugs'), and people (the 'wrong ones') gaining access to pathogens. More succinctly, and with a view to broader so-called "national security measures", biosecurity has been described as, "protecting biological resources against acquisition by terrorists" (Atlas 2005b, p. 122).

In each of these accounts, the general principle is the same – to keep 'dangerous tools' out of 'dangerous hands'. As David Franz, a senior biodefense scientist and former member of the Fink Committee, put it: the "classical" biosecurity model depends upon "guns, gates and guards" to restrict access to biological resources that might be "deliberately misused".

In this light, the 'classical' biosecurity model can be thought of as a type of 'command and control' strategy that depends upon maintaining a clear division between those who can and those who cannot 'legitimately' (and, in the case of 'Select Agents', legally) participate in aspects of modern biology. Typically a core component of arms control (including chemical and nuclear weapons) and environmental policy regimes, 'command and control', sometimes referred to as a 'direct regulatory instrument' (Goulder and Parry 2008), represents a 'top-down' approach to regulation, relying on the prohibition of undesirable behavior, which can be monitored and then enforced through national laws (Holling and Meffe 1996). More generally, 'command and control' has been described as an "approach to solving problems … in which a problem is perceived and a solution for its control

[53] See http://www.selectagents.gov/.

is developed and implemented" (ibid, p. 329). "Most of all," a command and control approach "is expected to solve the problem either through control of the processes that lead to the problem" (ex ante control measures) "or through amelioration of the problem after it occurs" (ex post control measures) (ibid.).

On the one hand, this would appear to be an exceptionally narrow framing of a 'problem' to be 'solved', reducing 'biosecurity' (as conceived under the 'classical' biosecurity model) to the level of isolating and restricting access to a select group of harmful biological entities. On the other hand, as the following accounts suggest, this framing is deceptively complex, and possibly open-ended. Commenting on the underlying principles of a 'command and control' approach to 'risk governance', Kwik et al. (2003), a group of biological weapons experts from the Johns Hopkins Centre for Civilian Biodefense Strategies, suggest:

> "This type of governance depends on being able to assign crisp edges to what is and is not subject to regulation, and the ability to define explicitly what is allowed and what, precisely, is prohibited." (Kwik et al. 2003, p. 30)

Or, as Holling and Meffe (1996, p. 329) suggest, a "command-and-control approach implicitly assumes that the problem is well-bounded, clearly defined, relatively simple, and generally linear with respect to cause and effect."

But, what if "these same methods of control are applied to a complex, nonlinear, and poorly understood natural world, and when the same predictable outcomes are expected but rarely obtained" (Holling and Meffe 1996, p. 329)? In the case of the life sciences and biotechnology, there are indeed no 'sharp boundaries' demarcating 'productive' from 'destructive' life science artifacts (McLeish and Nightingale 2007). Which begs the question: 'who' or 'what', precisely, is to be regarded as 'dangerous' or 'of concern' in the contemporary life sciences, and where should one draw the line? As I have suggested, the very concept of the 'dual-use dilemma' invites the possibility that *all* life science artifacts (biological or informational, tangible or intangible) *can* be dangerous and *might* be deliberately misused. In this context, there are no 'crisp edges' that can be used to define 'what is and is not subject to regulation' and 'what is allowed and what, precisely, is prohibited'. Therefore, although binaries, categories, lists, and labels may be

desirable from the standpoint of the 'classical' biosecurity model – a 'command and control' approach to regulation – as they serve to demarcate the boundaries of 'safe' and 'dangerous', 'legitimate' and 'illegitimate', 'right hands' and 'wrong hands', such divisions, in practice, do not exist. On the contrary, they are created.

4.2.4 Problematizing synthetic biology

It is, then, within this context that synthetic biology and synthetic biologists are embedded: a context that views 'bioterrorism' as a problem worth worrying about; one that endeavors to control 'dangerous tools' from reaching 'dangerous hands'; and one that is actively seeking to determine who or what, precisely, is to be regarded as 'dangerous' or 'of concern' in light of a 'dual-use dilemma' in the life sciences. As Drew Endy, a prominent American scientist who has been instrumental in shaping the underlying goals of, and possibilities for, synthetic biology, commented during an interview for my research:

> "This is the world we've inherited … there is an additional lens that shapes security conversations where there's quite a strong focus on sub-state actors and individuals. In this context, synthetic biology has garnered a fair amount of attention, in that if *anybody* could order up the genome, and perhaps bring to life a viable hemorrhagic fever … And so our political systems, or security systems, are prepared to respond to that. So, you can talk about the *impact* of synthetic biology on biosecurity grounded in the context of existing biosecurity practice and strategy." (Drew Endy)

Much of what I have said up to this point has been in an effort to acknowledge precisely this – 'existing [US] biosecurity practice and strategy' – so that I may discuss synthetic biology in context. This is because, synthetic biology does 'inherit a world', and it is one that frames biology and biologists in a highly specific way: it is a world of 'bioterrorism' and 'biosecurity', of 'dangerous tools' and 'dangerous hands'. It is a world of defense, of material controls, and of a ceaseless search for new 'vulnerabilities' engendered by advances in the life sciences. Thus, when conceiving of the 'how's' of risk-based government in synthetic biology, this

context must always be kept it mind, as it has, *fundamentally*, made the 'biosecurity problems' associated with synthetic biology 'knowable' and 'speakable', as well as orienting a "constellation of experts" (Rabinow 2008, p. 279) in their attempts at finding practical 'solutions' to seemingly intractable policy 'problems'.

In the following, I will explore how synthetic biology fits in this context – that is, how it is perceived to contribute to a growing list of contentious life science research; and how it is perceived to complicate the underlying aims of biosecurity, a defensive practice premised upon keeping 'dangerous tools' out of 'dangerous hands'. This research represents a contribution to the recent work of social scientists interested in asking how cutting-edge biotechnologies like synthetic biology are understood and represented as 'biosecurity problems', which are believed to merit some sort of regulatory response (for example, Collier et al. 2004; Lakoff and Collier 2008). Conceptually, this body of scholarship treats "bioterrorism and biosecurity as a site of problematization" (Collier et al. 2004, p. 3), exploring "how policymakers, scientists, and security planners have constituted potential future events as biosecurity threats, and have responded by criticizing, redeploying, or reworking existing apparatuses" (Collier and Lakoff 2008, p. 12). This approach, "places in question existing attention to risk and its modes of identification, recognition and definition" (Hutter and Power 2005, p. 11). Synthetic biology, I suggest, is undergoing a process of 'problematization', as both the science and its diverse practitioners are perceived to destabilize previous ways of understanding the world. The naming and classification of new 'risk objects' for regulatory attention (the subject of this chapter), I suggest, represents the first step in an ongoing risk management process that seeks to identify, and ultimately 'fix', regulatory gaps in biosecurity, enabling synthetic biology – as a science, an industry, and a source of seemingly boundless expectations – to move forward.

4.3 Taxonomy and the objects of classification

If labeling what is to be regarded as 'dangerous' or 'of concern' in the context of the contemporary life sciences is difficult, it is, perhaps, especially so with regard to

synthetic biology. This is because synthetic biologists claim to be able to achieve a qualitative change in modern biology: promising that more people in more places will be able to design and build 'novel biological systems'; promising to make 'new life' from component parts or 'off-the-shelf' chemicals; promising a rational, 'engineerable' biology that does away with complexity and the need for tacit knowledge, ushering in the much anticipated (yet unfulfilled) promise of a deterministic biology. Synthetic biologists, in brief, have promised much, and there are many ways of interpreting the scope and potential of their field. For those scientific and technical experts, sometimes referred to as 'biosecurity authorities' Mukunda et al. (2009), whose job it is to monitor and to remain a step ahead of so-called 'biosecurity risks', so that these risks may be assessed and managed, the interpretive flexibility of what synthetic biology is – or what it *could be* if synthetic biologists' expectations are fulfilled – provides a seemingly limitless pool of people and things to watch out for, to learn about, and to comprehend. Like other regulatory subject matter perceived to deviate from familiar methods of control, "[a]s new risk management needs arise, institutions develop new ways of categorizing, classifying, thinking, and acting" in an effort to reestablish order in the face of uncertainty and change (Ericson and Haggerty 1997, p. 25).

Thus, the task facing these experts is arguably a difficult one, requiring considerable knowledge about the diverse equipment, techniques, practices, and practitioners bound up with synthetic biology, all of which require sorting, naming, and prioritizing, so that a coherent picture of the 'synthetic biology threat' can be constructed. In many ways, this work resembles 'taxonomy' – a science that involves the meticulous identification and grouping of diverse elements, and an equally meticulous naming of structures, types and categories, so that order can be applied to disorder. Also like taxonomy, much of the work conducted by these experts draws on techniques concerned with seeing and contrasting minute differences between similar entities, as such differences suggest new categories of interest and concern. But, of course, biosecurity is not taxonomy. It works with different materials and with different aims. For diverse risk and security experts engaged in aspects of the synthetic biology regulatory response, perceived differences (between people and

between things) do not suggest, for example, new species delineations, but rather new vulnerabilities in a system of controls on select biological materials and information. Thus, for these experts, perceived differences – emergent and novel properties or characteristics – are, in many ways, synonymous with new 'problems' and 'risks', as they are perceived to expose 'gaps' in biosecurity.

There are, I argue, two principal branches that constitute, what might be called, the 'taxonomy of difference' that describes the 'synthetic biology threat'. First, there are the 'tools' that makeup the science, broadly defined as the assemblage of instruments, techniques, and knowledge that are said to enable the construction of 'new life' and 'novel biological systems'. Second, there are the 'hands', the actors who promise to make use of these tools in such a way that they may be used to circumvent the controls in place on certain kinds of biological materials and information deemed to be of greatest 'dual-use concern'. In each case, it is by way of 'marking out difference' – identifying and naming those aspects of synthetic biology and synthetic biologists that are perceived to be 'new' or 'novel' – that experts conceive of people and things as 'biosecurity problems' or 'biosecurity risks'. Taken together, these labels suggest an expanding taxonomy of 'dangers' and 'concerns', but one that lacks much of the coherency and hierarchical structure traditionally associated with taxonomy. That is, the structure of the 'synthetic biology threat' is non-linear, heterogeneous, and undergoing a process of definition. Indeed, much of the work of fixing boundaries – marking out a coherent space for thought and action – remains unresolved. Yet, it is with a view to this emerging taxonomy that one is provided with a glimpse of the emerging 'problems' and 'risks' that are presently attributed to synthetic biology, as well as how the science and its practitioners are presently framed as 'matters of (bio)security'.

4.3.1 'Dangerous tools': The problem of 'doing biology differently'

Synthetic biologists are often outspoken about the 'novelty' of their science.[54] In particular, they boast of an impressive range of tools that promise to make the design and engineering of biology easier and more widely accessible. For those experts whose job it is to identify and control emerging risks in the life sciences, these tools are (by virtue of the 'dual-use dilemma') often viewed with suspicion. Yet, it is not always clear what these 'tools' look like, and how, precisely, they might be problematic, which contributes to a variety of opinions on which are to be regarded as the most worrying and of greatest 'dual-use concern'. There are, for example, DNA sequencers and DNA synthesizers, which are physical laboratory apparatus that might be misused, and that might be identified and listed with minimal difficulty as 'dangerous' or 'of concern'. However, then there are DNA sequence libraries, registries of 'standard biological parts', and other online, information-based resources, which are more 'virtual' than 'physical', and perhaps less easily conceived and classified as 'dangerous' or 'of concern'. Finally, there are the more abstract aspects of synthetic biology, which do not (at least intuitively) resemble 'tools' at all, but are perhaps no less instrumental in making the science problematic: these are the foundational tenets on which the science is based – the methodologies and stated aims that set out the nature and scope of the field, and which arguably provide the field with much of its identity. Although discussed today, amongst life scientists and technologists, these methodologies are largely oriented to the future – that is, they are largely based on the promise of a truly rational, 'engineerable' biology, which might enable 'anyone' to design and build 'life

[54] They are arguably less so when responding to arguments that suggest their science is sufficiently 'new' to require an entirely new (possibly more burdensome) approach to regulating the materials and information they work with. That is, they are willing to express that synthetic biology is 'novel', but not *so* novel that it should demand exceptional regulation. Similarly, while synthetic biologists welcome discussion on the subject of synthetic biology's potential 'biosecurity risks', they are not prepared to assert that these risks are insurmountable. Aspects of these themes are touched on later in this chapter and discussed in further detail in subsequent chapters.

from scratch'. In the following, I will discuss how each of these 'tools' is framed (in part) as 'dangerous', and how each is perceived to pose its own challenges to naming and classification. In doing so, I will also highlight that notions of 'difference', and thus 'vulnerability', are applied equally (if not more so) to the 'non-physical' tools of a science that promises nothing less than a 'new way of doing biology' as it does to the 'physical' tools that more visibly characterize the field.

4.3.1.1 'Foundational technologies'

First, for some, including the Fink Committee (NRC 2004), as well as several experts interviewed for my research, "proliferation is over" (David Franz). By this statement, what these experts mean to suggest, in the words of the Fink Committee, is that, "it is futile to imagine that access to dangerous pathogens and destructive biotechnologies can be physically restricted, as is the case for nuclear weapons and fissionable materials" (NRC 2004, p. 23). In other words, in contrast to the scarce materials and technical infrastructure that characterize the nuclear field and the threat posed by nuclear weapons, physical pathogens and tangible biotechnologies are already "widely accessible, both to nations and to terrorist groups" (ibid.).

Yet, despite the assertion that 'proliferation is over' – a view that is arguably based less on the belief that physical pathogens and tangible biotechnologies cannot (much less should not) be controlled, and more on the belief that access to intangible life science knowledge is an equally (if not more) urgent problem (as I will discuss in relation to genetic sequence information following the present discussion) – this remains a problematic issue for many. Indeed, it is not uncommon for scientific and technical experts to represent tangible biotechnologies, exemplified by modern laboratory equipment, as 'intrinsically dangerous' (McLeish and Nightingale 2007). In this manner, laboratory equipment, chemical reagents, and other physical 'ingredients' for doing biology, are characterized as possessing a 'latent potential' for dangerousness, seemingly existing independently of human action. This characterization of biotechnology is especially apparent in an article

written by the biosecurity experts Kwik et al. (2003, p. 28), who refer to, "inherent risk in bioscience" and describe, "the kidnapping of modern biology".

Of course, irrespective of the intrinsic characteristics that are ascribed to modern laboratory equipment, it is ultimately not the 'equipment' that is perceived to be the problem, as equipment does not operate itself. Rather, the 'problem' is ultimately associated with what the equipment is perceived to 'enable' or what it 'makes possible'. In the case of synthetic biology, much of what the science is perceived to be, as well as much of what is perceived to be problematic about the science, is defined by the present, as well as *anticipated*, capacities of two related technologies: DNA sequencing and DNA synthesis. Although these technologies are not 'new' (in fact, they predate synthetic biology by several decades), they have taken on new life in the synthetic biology discourse, described by synthetic biologists as being faster, cheaper, and more productive than ever before (Garfinkel et al. 2007). As the microbiologists Wimmer et al.[55] suggest:

> "Unprecedented progress in synthesis and sequence analysis of DNA lies at the heart of the recent transformation of molecular biology and the emergence of the field termed synthetic biology." (2009, p. 1163)

Together, these so-called 'foundational technologies'[56] are perceived to make a specific thing possible, namely, 'synthetic genomics', a branch of synthetic biology that promises to 'read' (DNA sequencing) and 'write' (DNA synthesis) the four letter 'code' that comprises DNA, permitting the *de novo* synthesis of genes and genomes. Although I will not discuss the differing technical opinions about the limitations and operational difficulties associated with *de novo* synthesis or the problematic assumptions that underpin the belief that synthetic genes and genomes are akin to ready-to-deploy biological weapons (a subject I briefly touched on earlier in this

---

[55] The lead author on this paper, Eckard Wimmer, was also among the life scientists credited with creating 'synthetic poliovirus' (Cello et al. 2002), which is often cited as 'proof of principle' in terms of what is possible using this technology. This experiment, as I will discuss in Chapter 6, is one of several 'experiments of concern' that have recently helped motivate new US policy on 'dual-use research of concern'.

[56] This term has been used by synthetic biologists to describe those technologies "that affect the science and engineering of biology" (Endy 2005, p. 452).

chapter in relation to 'weaponizing' pathogens) at this time, as these are subjects that I will examine more closely in the last section of Chapter 6, what I do wish to discuss is how *de novo* synthesis is perceived to pose 'biosecurity problems' with regard to 'access' and 'classification' of dangerous pathogens.

The problem of access (in principle) is rather clear: DNA synthesis technology is perceived to permit the *de novo* synthesis of biological agents that are presently kept under lock and key ('Select Agents'). For those engaged in aspects of biosecurity policy, this is viewed as a singularly worrying problem, as it "might provide an effective alternative route to those who would seek to obtain specific pathogens for the purpose of causing harm" (Bügl et al. 2007, p. 628). What this means, in practice, is that in addition to guarding against the possibility of procuring pathogens from nature, from biodefense facilities, or from commercial culture collections, regulators must now also be concerned about pathogens being obtained through a combination of openly accessible DNA sequence information, off-the-shelf chemicals and hardware[57] – all of which are now framed as objects of 'suspicion' and 'concern'. Alternatively, and increasingly, companies that specialize in DNA synthesis are said to be able to provide the desired oligonucleotides (or 'oligos') (short stretches of non-specific DNA), genes or genomes 'on demand', and, as several experts interviewed for my research highlighted, "overnight".

The problem of classification, although less self-evident, is described as equally problematic in relation to biosecurity. This is because advances in synthetic genomics promise to make it possible not only to 'replicate' extant pathogens, but also to 'resurrect' ones that are extinct or 'create' entirely new ones. Thus, for some,

[57] Significantly, what is often missing from this equation is the individual with the requisite skills and know-how to actually make use of this technology. As the science and technology studies scholar Kathleen Vogel (2008a) observes, it is precisely this absence that obfuscates the social character of biotechnology while privileging *access* to materials and information. This observation is shared, as well as reinforced, by my own research, and will be returned to throughout my thesis. Discussing 'dangerous tools' independently of 'dangerous hands' in this chapter is, in part, intended to showcase the fact that the 'sociotechnical assemblage' (ibid.) that is synthetic biology, is, in fact, often divided into two separate hemispheres by experts, where materials and information are appraised quite independently of the people that might (mis)use them.

DNA synthesis undermines the very notion of a 'list' of controlled biological agents, as the following interview excerpts underline:

> "From the get go, I have been mystified … at the whole concept of a 'Select Agent List' because … with the ability to change existing pathogens or to build different kinds of pathogens, why focus just on these?" (Amy Smithson, chemical and biological weapons expert)
>
> "The thing that struck me most when I first learned about [DNA synthesis technology] was that this was going to change the landscape with regard to the Select Agent Rule. That lists were going to become obsolete." (David Franz)

As these accounts suggest, *de novo* synthesis is perceived to limit one's ability to categorically define (and ultimately control) a specific 'list' of pathogens, because modified pathogens or entirely new ones cannot be explicitly accounted for on a pre-existing list. The 'Select Agent List'[58] (introduced earlier) corresponds with a finite number of high-risk pathogens and biological toxins. It does not, and cannot, cover an infinite number of biological entities, especially ones that no longer exist, much less ones that have (perhaps) never existed. Thus, to the extent that experts believe in the potential of *de novo* synthesis to create 'new life', it is perceived to pose an open-ended 'biosecurity problem'. As Dana Perkins, the US public health official and biological weapons expert introduced in the previous section, expressed with regard to the limitations of lists in light of the possibilities enabled by synthetic genomics: "the range [of possible pathogens] expands so much that it may pose a challenge in terms of what we are preparing *against.*" This dilemma has similarly been voiced by a number of other scientific and technical experts (for example, Petro et al. 2003; Nixdorff et al. 2008; Mukunda et al. 2009).

In contrast, there are those who do not believe in the limitless potential of DNA synthesis technology and the open-ended capacity to synthesize new biological entities, and, for these experts, as one Australian biodefense scientist asserted during an interview at the BWC: "The claim, which has been articulated by some (mostly in the US context), that the Select Agent List is 'obsolete', because of the

[58] See http://www.selectagents.gov/SelectAgentsandToxinsList.html.

possibility of novel synthetic organisms, is absurd." Many, as I will discuss in further detail in subsequent chapters, share this biodefense scientist's objection to the notion that lists are 'obsolete', and their views are expressed in relation to, what they perceive to be, the most likely (not only 'possible', but also more or less 'probable') and/or the most relevant (in keeping with regulatory or other institutional norms) risks enabled by synthetic biology. For these experts, lists, although imperfect, remain practical instruments for delimiting the scope of high-risk pathogens with a view to keeping them 'locked up'.

Whether DNA synthesis technology will or will not make lists 'obsolete', it is nonetheless perceived to enable a larger universe of 'potentially dangerous' biological entities, if only by way of more readily enabling subtly different genetic constructs resulting in unfamiliar strains of existing microorganisms. And while simple modifications (for example, moving a single gene from one organism to another) have been possible since the advent of recombinant DNA technology in the 1970s, advances in DNA synthesis technology are described as making many more varieties of 'dangerous species' possible (for example, mixing and matching multiple genes from multiple organisms or inserting a novel 'synthetic sequence' into a naturally occurring one). Moreover, and of greatest relevance to the present discussion, as such microorganisms do not (yet) have names or known characteristics, they are, by some accounts, beyond classification, and thus quite literally beyond the remit of a 'list-based' approach to biosecurity.

4.3.1.2 'Sequences of concern' and 'malicious parts'

Second, the 'problem' of synthetic biology is equally perceived to be, as the Fink Committee observed in relation to biotechnology more generally (NRC 2004), a problem of the 'non-physical' aspects of the science. That is, the knowledge bound up with an improved understanding of biological processes and molecular life, increasingly communicated in the language of modern genetics. In particular, synthetic biology is closely tied to the production, distribution and use of genetic

information, either in the form of 'genomic sequence information'[59] or 'genetic parts'.[60] This information, encoded in the series of letters that represent the four base pairs that comprise DNA – adenine (A), thymine (T), guanine, (G) and cytosine (C) – is, for those who believe that biology can largely be reduced to genetic information (the dominant view conveyed by synthetic biologists, if complicated or contradicted in practice), itself perceived to be a powerful, and potentially dangerous, 'tool'. Unlike laboratory equipment, however, information does not possess physical properties that are readily observable and measurable, making it more difficult to define and control. Thus, from a biosecurity standpoint, genetic information is perceived to be especially problematic.

Many of the biosecurity concerns and dilemmas that are presently associated with the production and distribution of genetic information *vis-à-vis* synthetic biology are captured in the following quotation by Ronald M. Atlas, Co-director of the Center for Health Hazards Preparedness at the University of Louisville and former president of the American Society for Microbiology, who discusses the broader 'problem' of access to information in the context of the life sciences:

> "Beyond the issue of material control, i.e. how to prevent the acquisition by terrorists of dangerous pathogens, lies the more difficult issue of how to constrain information in the life sciences which is potentially dual use and could be misused to cause harm … But how can we define what is dangerous and how can we design a system that contains that danger while allowing legitimate biomedical research to proceed in a manner acceptable to society?" (Atlas 2005b, p. 133)

Atlas' question, "how can we define what is dangerous [with regard to information] and how can we design a system that contains that danger while allowing legitimate biomedical research to proceed in a manner acceptable to society?" is, for those

[59] See, for example, GenBank, "an annotated collection of all publicly available DNA sequences" that describes the genetic makeup of numerous genes and genomes (http://www.ncbi.nlm.nih.gov/genbank/).

[60] See, for example, MIT's 'Registry of Standard Biological Parts', a "collection of genetic parts that can be mixed and matched to build synthetic biology devices and systems" (http://partsregistry.org/Main_Page).

concerned about the deliberate misuse of synthetic biology, at the heart of much of their thinking and action. Like physical pathogens, information about pathogens (including sequence information associated with complex traits for pathogenicity and virulence) is perceived to pose problems of 'access' and of 'classification', threatening to undermine the 'classical' biosecurity model.

Concerns about access to genetic information are related to the belief that this information, once produced, is 'openly accessible' and thus 'vulnerable to misuse'. The availability of genetic information is described as being fuelled by rapid advances in DNA sequencing technology, which has permitted a growing number of genes and genomes to be 'decoded' and made available to a public audience via online genetic sequence databases. In the words of Mukunda et al. (2009, p. 7), a group of academic experts who have closely followed recent developments in synthetic biology with a view to its 'security implications', this information represents a "treasure trove of biological functions evolved during the more than 3.8 billion years since life on Earth began – a smorgasbord as it were, that invites experimentation and exploitation." The authors further emphasize that GenBank, the largest public database of genetic sequence information, "contains nearly 100 trillion letters of the genetic alphabet" (ibid.), offering "encyclopedic coverage of all the functional components and processes of organisms" (ibid, p. 8).

As this account suggests, concerns of this kind are interconnected with concerns about the accessibility of information over the Internet more generally. Like Mukunda et al, the security analysts Machi and McNeill (2010, p. 10) worry that, "the full genetic sequence for many select agents and other pathogenic genomes (smallpox, botulism, anthrax) are already in Internet-accessible databases that currently mandate free, unfettered, and anonymous access."[61] Furthermore,

[61] Contrary to Machi and McNeill's (2010) account, 'Select Agents' do not describe 'pathogenic genomes', but whole microorganisms. Moreover, 'genomes' are rarely 'pathogenic' in themselves. Rather, they must be inserted into a suitable cellular environment to be 'activated', a step that is more complex than synthesizing the genome itself (NSABB 2006). Again, these aspects of biological weapons development (in this case, the first step in a developmental pathway, as pathogens alone are not ready-to-

according to the French biological weapons expert Elisande Nexon (2011, p. 6), the "availability of genomic sequence data" becomes "more of an issue as capacities for [DNA] synthesis steadily increase", offering the possibility of the *de novo* synthesis of "virulence factors" and other genes "linked with a risk of misuse". Counter-bioterrorism specialists, Petro et al. (2003, p. 165), have voiced similar concerns about "digital proliferation", where sequence information, "commonly accessible via a currently non-attributable manner over the Internet", makes it "increasingly possible to reconstruct viruses from genomic digital data files".

On one level, then, concerns about access to genetic information would appear to be defined as much by advances in information technology (IT), as they are by advances in synthetic biology. That is, irrespective of its origin, sequence information, once put online, is perceived to be especially problematic, as the Internet enables 'unfettered' and 'anonymous' access. In this light, synthetic biology would appear to be problematic only in as much as advances in DNA sequencing technology have increased the quantity of genetic information available online, and advances in DNA synthesis technology make it increasingly possible to translate genomic sequence information into physical genomes. As the anthropologist Carlo Caduff (2008, p. 259) has rightly argued, many biosecurity concerns are not so much about "biotechnology's miraculous transformative capacity itself but rather the ability attributed to information to circulate and reproduce faster and more easily than matter." "Information", he suggests, "is bodiless, or is at least said to be so, and thus appears to escape the universal law of gravity" (ibid.).

On another level, however, synthetic biology does add a further dimension to existing concerns about access to genetic information, but this requires taking a closer look at another vision of the science and its possibilities, namely the so-called 'parts-based' approach to synthetic biology.[62] Under this approach, genetic

---

deploy biological weapons) are often glossed over in favor of generalized concerns about 'access' to intrinsically dangerous artifacts (McLeish and Nightingale 2007).

[62] Although the 'parts-based' approach to synthetic biology tends to be discussed in relation to synthetic biology's potential to make biology 'engineerable', which I consider following the present discussion, what I wish to emphasize here is that 'genetic parts', as

information is not characterized as a linear sequence of A's, T's, G's and C's, but as 'genetic parts' or 'modular parts', such as 'BioBricks',[63] which are intended to 'code' for specific biological functions. Synthetic biologists promise this will make genetic 'circuits' (coding, for example, for specific metabolic pathways) easier to assemble, analogized as snapping together Legos. Online databases, such as MIT's 'Registry of Standard Biological Parts',[64] store this information, which can then be used to synthesize desired biological components. Alternatively, these components can be ordered directly from the Registry, albeit many sequences and their corresponding DNA are presently described as poorly characterized, incomplete and/or unavailable.[65] The Registry is used by, among others, undergraduate biology teams during their preparations for the annual International Genetically Engineered Machine (iGEM) Competition, a competition that sees student teams from all over the world compete to construct innovative 'living machines'.[66]

For some scientists engaged in biosecurity policy, the concept of 'modular parts' is a problem in as much as it suggests a more flexible, standardizable, reproducible, bioengineering capability, offering new avenues for the proliferation and use of information that might be deliberately misused. As Richard Weller, a biological weapons expert and biodefense scientist working for the US Department of Energy, commented during an interview at the BWC:

> "If you have access to the genomic data [in the form of 'modular parts'] and the technology's advanced to the point where you sort of have this basic car frame ['chassis'] that you're now going to customize, you really don't need access [to pathogens]. I mean all of the things we have done, the time and energy and debate and everything we've done with regard to biosecurity (locking up bugs in a box or security facilities to prevent bugs from theft or diversion), it

---

specific configurations of genetic sequence information, are themselves perceived to be problematic entities in relation to the 'classical' biosecurity model.

[63] See the 'BioBricks Foundation', which describes 'BioBricks' as "the fundamental building blocks of synthetic biology" (http://biobricks.org/about-foundation/).

[64] See http://partsregistry.org/Main_Page.

[65] Ibid.

[66] See http://igem.org/Main_Page.

> becomes a sort of moot point, at least from an arms control or threat perspective." (Richard Weller)

Or, as Piers Millett, a biological weapons expert and senior administrator for the BWC, expressed this dilemma during an interview conducted for my research, in reference to intangible life science knowledge more generally:

> "From a proliferation perspective, it's no longer about locking up bugs; it's no longer about locking up materials or restricting the number of thermocyclers in the world or making sure that people don't have 1,000 liter fermenters in military facilities or whatever it is. Those points are going to be irrelevant, because the really dangerous stuff will be knowledge that you can't necessarily lock up." (Piers Millett)

Thus, for Weller and for Millett, and for many others who have, in recent years, voiced their concerns about the problem of access to intangible life science knowledge, the knowledge bound up with advances in synthetic biology is problematic not only because 'proliferation is over' (physical pathogens and laboratory equipment are already 'out there'); not only because this knowledge (communicated in the language of modern genetics and stored in online genetic sequence databases) is 'the really dangerous stuff', but also because, as Millett simply reasons, knowledge 'can't necessarily be locked up'.

The task of classifying the genetic information associated with synthetic biology, so that it can be characterized and monitored, is described as an equally (if not more) challenging problem for regulatory authorities. It is also more illustrative of scientific and technical experts' attempts at refining and inscribing notions of 'danger' and 'concern' at the level of knowledge about molecular life. Specifically, synthetic biologists' determination to make biology 'informational', breaking down cells into genetic 'circuits', 'parts', and 'parts of parts' that can be assembled in novel ways, pushes scientific and technical experts to locate their security concerns at the level of increasingly small units of molecular life, raising new questions and dilemmas. As Christopher Park, Senior Advisor for Bioterrorism in the Bureau of

International Security and Non-proliferation at the US Department of State,[67] contemplated with regard to characterizing smallpox in the process of moving from its 'scientific name' to 'strain' to 'genomic sequence':

> "What degree of genetic similarity does it need to have to some reference sequence to constitute smallpox? We have a law in the books that says 85 per cent similarity. Well, that's a problem, because some strains of monkypox in fact exceed that threshold. But they're not smallpox. So … we're getting to a point where these labels are not really adequate and useful tools, because where is the line? You know, once you move from form to sequence, you get the same problem as in evolutionary biology, where you start saying, you know, 'Do our species delineations make sense now that we're looking at sequences rather than bone structure?'" (Christopher Park)

In this account, 'labels', while perceived to be necessary, as they help differentiate between 'safe' and 'dangerous' genomic data, are seen as problematic. What 'constitutes smallpox' and thus a 'dangerous thing'? For this counter-bioterrorism specialist, the answer is not self-evident, and it is, perhaps, becoming less so with increased knowledge about molecular life. Specifically, he questions the utility of classifications based on marginal units of genetic similarity (or difference), compared to those based on species type, as it is no longer clear that this information uniquely characterizes the pathogen of interest and concern. Where is the 'threshold', and how does one know when it has been 'exceeded'? As Park expressed later: "the conclusion, at least for the moment, is, 'Yeah, there's a blurring, sorry. Use your best judgment'. It's not an easy problem to quantify." In this fashion, increasingly small margins of difference are used to demarcate those biological entities that are perceived to be 'dangerous' from those that are not, despite the practical difficulties encountered in making these distinctions.

---

[67] Please note: Christopher Park is now Director of the Biological Policy Staff in the Department of State's Bureau of International Security and Nonproliferation. However, throughout my thesis, I refer only to Park's professional responsibilities at the time of our interview.

Other interviewees expressed similar concerns, although voiced in slightly different ways. As one senior biodefense scientist, Volker Beck, remarked in the context of determining what constitutes a 'synthetic sequence', let alone a 'dangerous' one: "Where does synthetic biology start? Does it start with 15 base pairs, or does it start with 100 or 1,000?" Like Park, Beck expresses an ambivalent attitude towards meaningfully assigning a label to a marginal unit of difference. His question, roughly summarized as, 'at what point does a synthetic sequence begin to be conceived in terms of synthetic biology?' is arguably a good one, and one that would seem to be without a clear-cut answer. Yet, efforts are nonetheless being made to do precisely this. Specifically, although not discussed in the context of this interview, for the purposes of the first draft of the *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA*, a policy proposal put forward by the US DHHS (2009), which I will discuss in detail in the second half of the following chapter, the original recommendation was to only screen sequence orders of "200 base pairs" or more. In effect, this cutoff would then dictate when an order for 'synthetic DNA' (that is, a request for a physical strand of DNA produced using DNA synthesis technology and off-the-shelf chemicals; encoded on the basis of an arbitrary 'digital sequence' of A's, T's, G's and C's submitted by a prospective customer) begins to matter as a 'potential risk'. Some commentators described this decision as having "no firm, credible, or scientific justification" (Berger et al. 2010, p. 9). Upon further review, and based on feedback from a 60 day period of public comment, the DHHS (2010a, p. 3) agreed, deciding, "to eliminate the 200 bp limit" in the final draft because the "200 bp limit is not scientifically justified".

Synthetic biology, then, would seem to push the limits of classifying 'potential risks' at the level of genetic information. Yet, as the preceding discussion underlines, efforts are nonetheless being made to do so. In addition to the DHHS' (2010b) *Screening Framework*, the DNA synthesis industry is determined (albeit for different reasons, including averting commercial liability and more restrictive government legislation in the event of a biosecurity incident) to develop a curated, federally backed, list of 'sequences of concern' with which to compare incoming orders in an effort to screen out problematic sequences (Fischer and Maurer 2010). However,

even if it were possible to definitively 'know' which genes are 'dangerous' and which are not – an objective that is greatly complicated by uncertainty regarding gene sequence in relation to gene function, as well as complex interactions between gene expression and the cellular and extracellular milieu (NSABB 2010) – openly listing this information is said to be, from a biosecurity standpoint, potentially undesirable. As Piers Millett remarked with regard to the possibility of such a list:

> "There's a push towards gathering together all the information we know about pathogenicity and infectivity (all the ways in which pathogens act as pathogens) … But you're also therefore compiling a database of *exactly* the knowledge that would be of the greatest proliferation concern." (Piers Millett)

Or, as Christopher Park put it: "it would be a real cookbook for people doing things we don't want them to do." Others interviewed for my research raised similar concerns, contemplating the possibilities and difficulties of identifying and classifying 'genetic parts' that might confer virulence to otherwise harmless bacteria, referred to by several experts as "toxic parts" or "malicious parts".

Taken together, these accounts suggest that, to a growing list of 'dual-use biotechnologies', one might also add 'sequences of concern' or 'malicious parts' or any other configuration of genetic information that is perceived to be potentially hazardous. In this fashion, security concerns about synthetic biology contribute to the 'molecularization' (Rose 2001) of '(in)security', embedding notions of 'danger' and 'concern' in ever-finer parcels of molecular life. Although, as Herbert Gottweis (1998) has argued, a conceptual link between risk and (engineered) molecules can be traced to scientific and technical deliberations on genetic engineering in the 1970s, the 'risks' in question were of a different sort, reflecting a different set of political preoccupations and cultural concerns. Namely, genetic engineering was predominately framed as having potential 'unintended consequences', which were linked to concerns about the harmful (yet unintended) effects of emerging technologies (for example, nuclear power stations) on public health and the environment. Synthetic biology, in contrast, is framed as having the potential for 'deliberate misuse', reflecting more recent concerns, as I have suggested, about

bioterrorism. In brief, knowledge about molecular life (or at least *access* to this knowledge) is increasingly framed as a 'biosecurity problem'.

4.3.1.3 Biology made 'simple to engineer'

Finally, by some accounts, synthetic biology's 'methodology' is perceived to be the most problematic 'tool' of all. In this instance, biosecurity concerns are linked with the foundational tenets of synthetic biology itself, an emerging science characterized by a different way of thinking and talking about biology and biological research. According to Drew Endy (2005, p. 452), a key figure in the rhetorical structuring of this new approach to 'doing biology', synthetic biology depends upon "foundational technologies based on ideas of standardization, decoupling and abstraction" that "help make routine the engineering of synthetic biological systems that behave as expected". These concepts (and the related ideal of 'standard biological parts') graft the mechanical logics and vocabularies of engineering onto the more unruly substrate of biology – both the science and the material entity – suggesting the possibility of enhanced control over life. According to Endy, and others who share his vision, the hope is to set a new standard in pursuit of an ambitious experimental aim: to verify if biology can be made 'simple to engineer' (ibid.).

For scientific an technical experts engaged in biosecurity policy, while the possibility of a biology that is 'simple to engineer' is perceived to be promising, it is also perceived to be "a potential game changer" (Piers Millett). Biosecurity, as I have discussed, is premised upon keeping 'dangerous tools' out of 'dangerous hands'. Synthetic biologists' stated aims threaten to undermine this practice, calling into question the very logics of a 'command and control' approach to securing biotechnology. As Piers Millett explained during an interview:

> "It's not that synthetic biology *could* do this [enable broad-based bioengineering capabilities], but that its deliberate *intent* is to do this. Its stated aim is to allow more people to have access to biology; to turn it into an information science; to spread it around the world; to bypass technological

> requirements, and to reduce the time it takes from having an idea to a commercial application." (Piers Millett)

For Millett, and for others who embrace the possibilities enabled by this new methodology, synthetic biology signals something different because:

> "It's not a development. It's not a technological improvement. It's not the next step in a development chain. For me, at least, it is a genuinely different approach to biology, and one that will *fundamentally* change the space in which the security community works." (Piers Millett)

Here, a "genuinely different approach to biology" suggests 'genuinely different demands on securing biology', because, Millett reasoned, "security concerns ultimately do not come from small issues, they come from changing the way biology is done, and that leads me to a very different set of problems."

Mukunda et al. (2009, p. 13) have similarly argued that synthetic biology is unique to the extent that it "includes, as a principal part of its agenda, a sustained, well-funded assault on the importance of tacit knowledge to bioengineering and thus on one of the most important current barriers to the production of biological weapons." Based on interviews with "leading synthetic biologists" and "practicing biosecurity authorities" (ibid, p. 1), the authors suggest that, even though "the aspirations of Synthetic Biologists remain largely unfulfilled" (ibid, p. 3), the very possibility that synthetic biology *could* make biology easier to engineer is enough to set the science apart from earlier attempts at bioengineering and to make it of greater concern to many who are closely monitoring its development. With a view to these potential advances, as Mukunda et al. (ibid.) suggest, one can see that, if only setting a new 'agenda' and foreshadowing enhanced bioengineering capabilities, synthetic biology is, for some experts, both exceptional and worrying.

Yet, others are skeptical that synthetic biology signals a radical change in our ability to 'do biology'; highlighting that, even for those with considerable skill and know-how applied to constructive research projects, 'doing biology' remains a difficult job. David Franz, who was previously the head of the US Army Medical Research Institute of Infectious Diseases (USAMRIID), explained:

> "I always say that anything is *possible*. We can't afford to say, 'that's *im*possible; you'll never do that', or something like that. … On the other hand, I've tried myself or been around people who have worked on doing things with biology for so many years … it's *really* complicated. … And I remember all the *good* things we've tried to do, and how hard it is to do good things, as well. So, it's kind of humbling to see how little we really do know; and how little control we really do have of biology." (David Franz)

During my interview with Dana Perkins, she similarly emphasized that synthetic biology is not "Pasteur's microbiology". Perkins then went on to describe the specialized equipment, laboratory facilities, and alike, that she believes are necessary components for doing advanced bioengineering work. At the same time, her account was not without contradiction, responding to, "Will doing biology or synthetic biology ever be 'easy'?" with:

> "Well, biology's easy *now*. It's just that you'll have, in the future, synthetic biology made easy. And, in some respects, at the low-end, synthetic biology is *already* easy. It's just at the upper end, you know, where the areas of concern start, when you start to create completely new organisms..." (Dana Perkins)

Similar inconsistencies in individual accounts were not uncommon in the interviews conducted for my research. Frequently, experts expressed ambivalent attitudes about what synthetic biology 'makes possible', torn between understandings of what they believe the science can achieve *today* versus what they believe the science might enable in the *future*. This ambivalence was clearly discernable in an interview with Special Agent You of the Federal Bureau of Investigation's (FBI) Weapons of Mass Destruction Directorate. According to Agent You, a virologist by training and now a leading figure in the US government's biosecurity awareness raising activities directed at synthetic biologists (and life scientists more broadly), although synthetic biology may not pose an "immediate threat", it is important to not "fall behind the curve", as "this is going to be the century of the life sciences, potentially." Drawing the common analogy between IT (or 'computing') and synthetic biology, Agent You argued that, if the "security community" had sufficient foresight in the 1970s,

> "we wouldn't be so behind the curve now when it comes to your information getting hacked or identify theft or getting your system infected by a virus or a worm, and all those sorts of issues. I mean, if we had acknowledged that those could be possibilities, back then, systems would be much better protected now. So, if we take a lesson from history … then it's incumbent upon us to have these discussions now [about synthetic biology and its potential risks], so that we're not behind the curve yet again." (Edward You)

Significantly, Agent You's assessment is not just based on his own premonitions about an emerging science and its potential risks. Rather, it builds on the expectations of synthetic biologists, who claim that advanced "capabilities" in synthetic biology are inevitable, often comparing their science's trajectory with the history of "computing" (interviews with Andrew Hessel and Rob Carlson). In reference to the outlooks of two prominent synthetic biologists, You reasoned:

> "If we take the visions of Andrew [Hessel] and Rob [Carlson] seriously – saying that's where they see the future, where they see households rather than companies and universities having these capabilities – then there is a need for the security community to be proactive and to act now." (Edward You)

In this light, even though biosecurity experts like Agent You believe that synthetic biology currently falls short of its stated aims, and that there are not yet 'DNA synthesizers in every home' (a common claim made by synthetic biologists about the future of their science, anticipated by Hessel and Carlson), there nonetheless exists the possibility that the expectations of leading synthetic biologists could be fulfilled. Moreover, if these expectations are fulfilled, and if the IT experience can provide a meaningful point of comparison and a historical lesson, it is important to 'act now' in anticipation of just such a technological future.

Ambivalence of this kind, I suggest, can be traced to the 'anticipatory' nature of threat assessments and risk forecasts more generally, which endeavor to look forward; yet must be based on existing data and present beliefs. Uncertainty, in other words, is not only intrinsic to possible future events, but also to the manner in which these events are imagined (O'Malley 2004). As the science and technology scholar Kathleen Vogel (2008b) rightly argues, bioweapons threat assessments

attempt to imagine future threats based on current capabilities, limited 'intelligence information', and expected technological developments. Drawing on Stephen Hilgartner's (2007) analysis of 'anticipatory knowledge' in various arenas of biotechnology, Vogel underlines that assessments of this kind are "used to construct societal narratives about the future of biotechnology and the life sciences", which, in turn, drive "particular policy responses" that "flow from these narratives" (Vogel 2008b, p. 562). Thus, when synthetic biology's 'potential risks' are linked to claims about uncertain technological futures, there exists considerable scope for ambivalent or contradictory assessments about the 'risks' that are to come. In turn, there exists considerable scope for multiple 'policy responses'.

There is, of course, no way of knowing whether synthetic biologists will achieve their stated aims and successfully implement a 'new way of doing biology'. By some accounts, a future of this kind would appear to be doubtful. In an article entitled, 'Five hard truths for synthetic biology', published in the journal *Nature* in 2010, Roberta Kwok argues that, although "some accounts of synthetic biology" seem to be "restricted only by the imagination" – inspired by visions "that biologists can extend genetic engineering to be more like the engineering of any hardware" – analogies of this kind "don't capture the daunting knowledge gap when it comes to how life works" (Kwok 2010, p. 288). In other words, for Kwok, and for others who remain skeptical of Endy's (2005) vision for synthetic biology, which is in effect a vision for the future of biological research and bioengineering more generally, biology is not, and moreover may never be, 'simple to engineer'.

Yet, despite this more modest outlook on synthetic biology, for the scientific and technical experts interviewed for my research, and for the majority of those I have encountered in the biosecurity policy literature, the *possibility* of an 'engineerable' biology is taken seriously; it is factored into their 'anticipatory gaze', and composed as 'anticipatory knowledge' about "a future that may never happen but that must be guarded against" (O'Malley 2004, p. 7). In the absence of evidence about the capacities and potentials of an emerging technology (and amidst a host of uncertainties about the actors who might choose to misuse this technology), 'if, then' thinking becomes central to both synthetic biologists' claims about their science and

to 'biosecurity authorities' (Mukunda et al. 2009) concerns about its potential for 'deliberate misuse'. Thus, irrespective of whether the future will coincide with a biology that is 'simple to engineer', few would seem to discount that such a future is at least possible. And, "if it is possible", as the authors of a report on synthetic biology and its implications for insurers suggest, "then there is a risk" (Lloyd's Emerging Risks Team 2009, p. 10, section: "What could go wrong?").

4.3.2 'Dangerous hands': The problem of 'being a different kind of biologist'

For many scientific and technical experts, as I have suggested, a 'democratized' biology is perceived to be a dangerous biology. Moreover, it is perceived to be 'dangerous' in a highly specific sense – namely, it is said to have the potential to enable more people to gain access to biological materials and information that have traditionally been kept out of reach of those outside familiar (secure) research settings. Whether enabled by DNA synthesis technology, the availability of online genetic sequence information, or a methodology that promises a more inclusive bioengineering capability, the perception that synthetic biology does (or *will soon*) lower barriers to access invites the possibility of new actors taking part in potentially dangerous biological research. But, which actors, precisely, should be the subjects of concern? And, what is it about these actors, in particular, that is perceived to be especially problematic? As the editor-in-chief of the journal *Nature* queried (Campbell 2006, p. S19) in 2006, while it is possible that someone might choose to use synthetic biology for 'malign purposes', "who might that malign someone be?" For biosecurity experts, who are sought for their knowledge on the kinds of people who are likely to engage in acts of bioterrorism, these questions are increasingly central to their professional responsibilities.

In the following, I will argue that just as experts engage in a process of selection to name those tools associated with synthetic biology that they perceive to be of greatest relevance and concern, they similarly engage in a process of selection to determine who might misuse these tools. For these experts, perceptions of 'difference', once more, suggest new vulnerabilities, but, in this context, the

perceived differences are not between things, but between people. Specifically, it is with a view to a 'different kind of biologist', one who is empowered by the tools of synthetic biology and who works on the margins of 'institutional science', that many security concerns are grounded. People, unlike things, however, interact with the names that are applied to them, and, thus, the act of naming and classifying a 'dangerous person' poses problems and dilemmas beyond the practical difficulties associated with the naming and classification a 'dangerous thing'.

4.3.2.1 The 'spectrum of potential attackers'

Given the "spectrum of potential attackers" (Moodie 2009, p. 14)[68] who might deliberately misuse synthetic biology, how are biosecurity experts to determine who is of greatest relevance and concern? The answer (and for those engaged in assessing the risks posed by modern biology there must be an 'answer', as their work requires that one is found) is that not everyone counts equally. There are, in brief, some hands that are perceived to be more dangerous than others. And, while determining who, precisely, these 'hands' belong to would seem to be an open-ended problem, the 'spectrum of potential attackers' has, in fact, already been narrowed down considerably; by the nature of the 'concerns' themselves.

As I have said, to speak of 'bioterrorism', and not of 'biosafety' or of 'biowarfare' or of much else besides, is already to suggest certain possibilities while obfuscating others. That is, concerns about bioterrorism suggest a particular kind of problem: one that pertains to the activities of sub-state groups or individuals intent on using biology to cause deliberate harm, saying nothing about the risks arising from laboratory accidents or the activities of states. As one synthetic biologist put it during an interview: "The *only* concern that is legitimate, in many people's minds, is

[68] I should note that the phrase, 'dangerous tools in dangerous hands', which is a key theme introduced in this chapter, was partly inspired by the title of Moodie's (2009) report, 'Dangerous weapons in dangerous hands: Responding to the Challenges of Chemical and Biological Terrorism'. However, other than this similarity, my research does not conceptually overlap with Moodie's (a consultant on international security affairs). In fact, the terms, "Dangerous weapons" and "dangerous hands" appear only in the title of Moodie's report and are not developed as concepts (ibid.).

from non-state actors, from terrorists ... The 'bad guy' isn't a state anymore; it's non-states." Here, concerns about '(bio)terrorism' are perceived to limit the scope of who can and should be reasonably worried about. So much so, that the activities of '(bio)terrorists' are, in many ways, perceived to be the only activities worth talking about. This view reflects a common apprehension (particularly among those working outside the US regulatory context) about contemporary biosecurity policies that increasingly prioritize the non-state threat over other (potentially more important) problems, including biowarfare and biosafety.[69]

However, unlike many contemporary security discourses, the synthetic biology biosecurity debate tends to focus not on the clandestine activities of foreign 'terrorists', but rather on the relatively visible activities of the diverse practitioners that makeup the 'synthetic biology community'. And perhaps one should not be surprised that this is the case. Synthetic biologists are, after all, the ones doing the research, driving the technology forward, generating innovative ideas, and generally interacting with the materials and information bound up with the science, all of which can (in principle) be deliberately misused. As the biological weapons experts Tucker and Zilinskas (2006, p. 40) argue: "In any large population of professionals, a small minority may be prepared to use their skills for illicit purposes." In the case of synthetic biology, as of 2006, they suggest that:

> "The pool of people capable of misusing synthetic biology is currently limited to the small number of undergraduates, graduate students, and senior scientists who constitute the research community – probably fewer than 500 people … In the future, however, the number of capable individuals will grow

[69] During the course of the interviews conducted for my research at the BWC, a number of biological weapons experts, mostly based in Europe, expressed concerns about the emphasis on bioterrorism in the US context, suggesting that bioterrorism tends to overshadow, what they perceive to be, the more immediate problem of state-level biological warfare programs, which are perceived to currently have the necessary resources to make use of synthetic biology for hostile purposes. At the same time, concerns about bioterrorism *vis-à-vis* synthetic biology are not absent outside the US, but rather tend to be viewed as one among a number of possible risks (see, for example, Parliamentary Office of Science and Technology 2008).

> rapidly as researchers are drawn into this exciting and dynamic field." (Tucker and Zilinskas 2006, p. 42)

Thus, when selecting and naming 'potential attackers' who might misuse synthetic biology, biosecurity experts tend to look first to members of the 'synthetic biology community' for answers. According to Gerald L. Epstein (2008), a security expert and Director of the Center for Science, Technology, and Security Policy at the American Association for the Advancement of Science: "Terrorists becoming biologists is less of a concern than biologists becoming terrorists",[70] underlining the belief that 'being a biologist' is not only a profession, but also a craft, which is perceived to enable certain possibilities and engender certain risks.

Synthetic biologists, too, have been outspoken about the possibility of their science being deliberately misused by members of their own community, and, in some cases, they have gone to considerable lengths to share their concerns with others. Writing in the journal *Nature* in 2005, for example, George Church, a geneticist at Harvard Medical School and a leading figure in synthetic biology, called for not only a "code of professional ethics for synthetic biologists", but also for a variety of modes of monitoring and surveillance that might be used to "watch out for the rare cases when they transgress" (Church 2005, p. 423). According to Church, synthetic biologists must learn from past experience (that is, the history of previous technologies) and "should imagine worst-case scenarios and protect against them", including through the development of a variety of 'technical solutions' that would prevent engineered pathogens from causing harm if released into the environment (a subject that I will discuss further in Chapter 6) (ibid.).

Like Church, a number of the synthetic biologists (Drew Endy; Rob Carlson) interviewed for my research expressed their long-standing commitment to biosecurity and their early advocacy for 'biosecurity awareness' within their community. Moreover, and lending support to these accounts, a number of

[70] This view was similarly expressed at a workshop that I attended during my field research, when one commentator argued that: "It is more likely that a biologist will become a terrorist, than a terrorist will become a biologist" ('Microbiology, genomics and beyond: Regulating dual use technology into the 21st Century Programme', held at the Wellcome Trust, London, 17 September 2010).

biosecurity experts (Richard Weller; Edward You) interviewed for my research emphasized that their concerns about synthetic biology were in fact motivated by the voiced concerns of several prominent synthetic biologists (notably, Drew Endy and Rob Carlson). In other words, in some cases, synthetic biologists would appear to have raised 'biosecurity concerns' about their science (and their 'community') before biosecurity experts were aware of 'concerns' to be 'concerned about'.

However, synthetic biologists' advocacy for safety and security can equally be understood as an attempt to underline a commitment to 'responsible science', preempting public concern and potential controversy. According to Church (2005, p. 423): "Whether we believe that these are immediate, distant or imaginary threats, the concerns are real." Here, Church would seem to suggest that he is no less concerned about the 'concerns about the risks' than he is about the 'risks' (the material ones) themselves. In reference to the legacy of genetically modified products and gene-therapy drugs, Church further cautions against failed exercises in public engagement (ibid.). Accounts of this kind reveal that, more than ever before, scientists are acutely aware of the 'secondary' or 'reputational' risks that go hand-in-hand with managing the 'primary' risks that are the immediate subject of regulation (Power et al. 2009). In this light, although advocating for a commitment to biosecurity, Church (and the synthetic biologists noted above) would appear to be no less concerned about, and preoccupied with, demonstrating a sense of responsibility and maintaining an air of optimism about their science. Indeed, Church (2005, p. 423) concludes his article on precisely this note: "Finally, the community needs to discuss the benefits of synthetic engineering to balance the necessary, but distracting, focus on ['primary'] risks." Whether motivated primarily by concerns about bioterrorism or primarily by concerns about a loss of public support for their research, the fact remains: synthetic biologists have been among the first to declare that their science could be deliberately misused.

Yet, even in light of general agreement that the 'synthetic biology community' is itself a source of potential concern, there remain further difficulties facing those engaged in determining who is worth worrying about within this community. In particular, there exists a lack of clarity about *who* makes up the 'synthetic biology

community' to begin with; and, moreover, what it means to be a 'synthetic biologist'. Synthetic biology is often described as an interdisciplinary 'field', bringing together life scientists, chemists, engineers, physicists, computer scientists, materials scientists, and others (Schmidt 2008; NSABB 2010). These actors, in turn, are engaged in a diverse range of activities, "driven mainly by the idea of turning biotechnology into a true engineering discipline" (Deplazes 2009, p. 428). In brief, synthetic biology is framed as many things; synthetic biologists as many people, and, together, they are loosely clustered around an 'idea' – that is, to make biology 'engineerable'. For even the most 'category-inclined' regulator, making sense of these diverse elements might justifiably be described as 'daunting'. For several of the biosecurity experts interviewed for my research, the ambiguity surrounding synthetic biology was simply described as "fuzzy". Therefore, although concerted efforts are being made by biosecurity experts (among others) to make sense of synthetic biology – mapping out those aspects of the science and its practitioners that make it distinctive – 'knowing' with any degree of clarity what 'synthetic biology' is and who constitutes the 'synthetic biology community', let alone who within this community might be 'dangerous', remains highly uncertain.

4.3.2.2 Outliers and exceptional cases: 'Lone wolves' and 'biohackers'

Despite these uncertainties, however, efforts are nonetheless being made "to anthropomorphize danger and construct a vision of the enemy", which is a defining feature of any security regime (Bigo 2006, p. 22). Like other security regimes, the synthetic biology biosecurity discourse also draws on notions of 'otherness' to demarcate those who are and those who are not to be regarded as 'real' or 'legitimate' threats to our collective security. In particular, it is with a view to those working on the margins of synthetic biology – the outliers and exceptional cases – that new categories of 'dangerous person' are in the process of being produced. At the heart of this process of selection and classification are biosecurity experts' perceptions of synthetic biologists' idealized goals, which promise, on the one hand, "to eventually expand the universe of capabilities open to its [synthetic biology's]

most skilled practitioners", while, on the other, "substantially leveling the gradient between elite and peripheral practitioners" (Mukunda et al. 2009, p. 15). In each case, synthetic biology is perceived to have something to offer the small fraction of those who would choose to deliberately misuse the science.

For 'elite practitioners', the full potential of synthetic biology is perceived to be at their disposal, inviting an array of possibilities that might undermine current biosecurity efforts. Variously referred to by biosecurity experts as 'lone operators', 'lone wolves' or simply 'scientists with a grudge' (Tucker and Zilinskas 2006), this type of person is perceived to be someone with ready access to the biological materials and knowledge that form the basis of synthetic biology, which they can, in turn, use to design and build (given the current 'state-of-the-art') just about any dangerous pathogen.[71] In many ways, this person might be any 'synthetic biologist' who, working on the margins of 'legitimate' life science research, chooses to use this research in 'illegitimate' ways. For example, according to Gerald L. Epstein:

> "The most serious potential scenario would be if individuals trained sufficiently broadly in biological science or biotechnology – and who therefore already have the expertise to develop biological weapons – become sympathetic with or recruited by terrorist groups." (Epstein 2008)

Once again, Epstein's views reflect the belief that experienced scientists possess privileged knowledge that can (in principle) be deliberately misused. This view, of course, is characteristic of 'dual-use concerns' more broadly, and has therefore done relatively little to destabilize perceptions of the 'dual-use threat'.

In the case of synthetic biology's 'peripheral practitioners', however, the problem is perceived to become markedly more complex. This is because synthetic biology promises to make it easier for 'less skilled' practitioners, formally excluded from 'institutional science', to participate in 'potentially dangerous' research, a

[71] Once again, this view is based on the assumption that *access* to materials and knowledge is itself a sufficient requirement for producing pathogens and viable biological weapons. As I have touched on earlier in this chapter, and as I will discuss in further detail in subsequent chapters (especially the final section of Chapter 6), this assumption fails to account for the practical difficulties (both technical and social) that complicate the research process.

scenario fundamentally at odds with current approaches to biosecurity (NSABB 2010). The 'classical' biosecurity model, as I have discussed, relies on barriers to access and distinctions to be made between those who can and those who cannot 'legitimately' participate in aspects of modern biology. But, what happens when these barriers are lowered, the line between 'legitimate' and 'illegitimate' practitioners blurred, and those formally excluded from 'institutional science' enter the field of play? As Piers Millett expressed during an interview:

> "Whilst I'm sure 99.9 per cent of those people would want to have fun; would want to make money; would want to get the Nobel Prize; would want to do something that was generally beneficial, you can guarantee down to human nature that some tiny little fraction will want to do something nasty with it." (Piers Millett)

Or, as Christopher Park succinctly put it: "You give the same technology to enough people and *somebody's* going to do something stupid." Like many biosecurity experts, Park and Millett (despite their optimism for the science and its potential) are concerned about the implications of giving more people the capability to engineer biology. The reason being, even though most 'peripheral practitioners' are expected to have good intentions, there are also those who might transgress community norms. And, for these experts – who are responsible for, according to the demands of their individual professions, imagining the unexpected and unwelcome possibilities enabled by modern biology – these are precisely the individuals (however few there may be) who are of greatest relevance and concern.

Of particular interest and concern is a growing community of amateur biologists or so-called 'biohackers', who seek to move biology and biotechnology out of 'institutions' and into garages, kitchens, basements, community labs, and other 'non-institutional' research settings (interview with amateur biologist, Jason Bobe, introduced in further detail below). The French biological weapons expert, Elisande Nexon (2011), offers a glimpse of the world of 'DIY-biology', as imagined from the perspective of security experts and life science regulators:

> "When considering biosecurity and biosafety, a new phenomenon is worth monitoring: namely, the emergence of 'do it yourself (DIY) biology' (also

> referred to as 'garage science'). The reduced cost and wider availability of specialist equipment and the spread of information have allowed citizen scientists and amateur biologists to practise biology outside traditional professional settings, including extracting and building synthetic DNA sequences in makeshift laboratories. Online networks such as DIYbio.org and OpenWetWare.org provide information and facilitate communication in ways that can lead to innovation, but that also represent a new challenge in terms of awareness, best practice and regulation." (Nexon 2011, p. 4)

Here, DIY-biology is framed as a distributed (online) network of 'citizen scientists' engaged in the very practices that are of greatest concern to those monitoring advances in biotechnology and developing biosecurity policies.

Although some question the extent to which amateur biologists are doing 'synthetic biology', as opposed to more basic forms of research conducted in its name (interviews with biological weapons experts and senior biodefense scientists at the BWC), their aims – to introduce modern biology into the public sphere – are intimately bound up with the promise of a science that seeks to make the manipulation of genomes 'user-friendly' by reducing the need for scientific and technical knowledge (Smith and Davison 2010) and 'black-boxing' "powerful applications" and "key procedures" (Chyba 2006).

In many ways, DIY-biologists, including artists, designers, hobbyists, and a handful of professional scientists (interview with amateur biologist, Mackenzie Cowell, introduced in further detail below), serve as a test case for what might be possible if synthetic biologists can (in time) make biology 'simple to engineer'. Moreover, from a biosecurity standpoint, the extension of biology to more people in less formal research settings is decidedly problematic. As one recent report by the US National Science Advisory Board for Biosecurity (NSABB) explains:

> "[S]ince current biosafety and biosecurity paradigms address life sciences research conducted at research institutions, there may well be gaps in oversight resulting from the large numbers of synthetic biology practitioners who come from backgrounds that are not traditionally considered life sciences or who lack formal institutional affiliations." (NSABB 2010, p. iii)

As the NSABB suggests, amateur biology is perceived to be a problem because, in brief, it is 'different'. That is, 'non-institutional biology' is perceived to be at odds with an existing regulatory 'paradigm' that is premised upon limiting access to 'potentially dangerous' life science research. In this light, to the extent that synthetic biology expands the number of users of modern biology, as a recent report by the Presidential Commission for the Study of Bioethical Issues (PCSBI 2010, p. 8) suggests, "synthetic biology poses some unusual potential risks".

On one level, concerns about 'amateur biologists' are essentially the same as those leveled at 'elite practitioners' – that is, synthetic biology might enable them to obtain dangerous pathogens. However, on another level, the concerns are qualitatively different. As the previous accounts suggest, concerns about amateur biology, in many ways, are not so much about *what* amateur biologists might do with synthetic biology (obtain dangerous pathogens), as they are about *where* they (or *where they do not*) conduct their work, and, ultimately, about *who* amateur biologists are (or *who they are not*). That is, amateur biologists are framed as something *other* than 'traditional life scientists' working in venues *other* than 'traditional research settings'. In this way, amateur biologists are defined by their 'difference' or 'otherness' in relation to 'life science proper'. And while these distinctions might, on the surface, seem to suggest little more than an alternative system of classification (one based on 'where' and 'who', and not on 'what'), under closer examination they reveal that, by labeling amateur biologists in this manner, experts are shaping and aggravating perceptions of their community.

For the co-founders of DIYbio,[72] one of the most visible communities of amateur biology activity, the pairing of amateur biology with concerns about 'bioterrorism' and 'weapons of mass destruction' (a connection made predominately, if indirectly, by the FBI's Weapons of Mass Destruction Directorate, which engages in a variety of biosecurity outreach and awareness raising activities related to synthetic biology) has significant implications for how members of their community are understood by others, as well as how they understand themselves (a

[72] See http://diybio.org/.

subject I will discuss further in Chapter 7). As Jason Bobe, co-founder of DIYbio, describes amateur biologists' ambivalent relationship with the FBI (and the omnipresent subject of 'WMD'), "as long as I can remember talking about DIYbio, it's always been about biosecurity and weapons of mass destruction", and about how "DIYbio offers a new avenue for terrorists to get access to weapons of mass destruction". Although Jason Bobe acknowledges that the attention that DIYbio receives in policy circles and in the media is testimony to their success (their community has grown considerably and is now, he suggests, "on the radar"), it is not exactly the kind of 'attention' they were looking for. "If you've heard of DIYbio recently", Jason Bobe explained (somewhat humorously) at the outset of his presentation at a workshop[73] interested in the 'dual-use' aspects of biotechnology, "it was probably in the context of weapons of mass destruction".

Jason Bobe and Mackenzie Cowell, fellow co-founder of DIYbio, have a vision for amateur biology; one that is geared towards,

> "making this simple, easy to use tool kit, based on synthetic biology, to tinker with biological systems, because [amateur biologists are] fascinated by that. But that 'tinkering tool kit', is not necessarily … going to enable you to build weapons or anything … It will let you play around with biological systems ... It will give you the intuition you need to engineer something in the future."

Thus, for them, amateur biology is about 'tinkering', about 'play', and about gaining 'intuition' about engineering biology. It is not (or at least not yet) about working 'on the cutting edge' and it is not about 'making weapons'.

In contrast to the dominant biosecurity frame that concerns itself with the problem of 'being a different kind of biologist' – one who operates outside the controls in place on institutional science – Jason Bobe and Mackenzie Cowell suggest that, "being a biohacker isn't so much about where the work is done or whether or not they're professionals or amateurs or artists or whatever, it's more about what the activity is". Thus, for them, the 'dual-use dilemma' is perhaps not the best way to frame synthetic biology (or at least their vision for synthetic biology) because, as

[73] 'Microbiology, genomics and beyond: Regulating dual use technology into the 21st Century Programme', held at the Wellcome Trust, London, 17 September 2010.

they suggest, "biology is really 'poly-use' and framing it as either 'good' or 'bad' overstates the clarity with which biology is practiced."

4.4. Conclusion

What is often missing from experts' accounts about the 'biosecurity risks' engendered by synthetic biology is that these 'risks' are neither innate nor inevitable. They are, in fact, contextually situated and largely contingent upon the statements made by diverse experts who compete to lay claim to what should count as a 'real' or 'legitimate' threat to our collective security. There are many ways in which synthetic biology could have been (and, indeed, still can be) framed as 'problematic', each presupposing particular kinds of worries, dilemmas and possible future harms. To speak of synthetic biology in relation to 'bioterrorism' and in accordance with the norms and logics of 'biosecurity' is to privilege one way of looking the world, while obfuscating many others. In this chapter, I have endeavored to think critically about how this highly specific framing permits synthetic biology to be understood and represented as a specific kind of problem for risk management. Synthetic biology, I have suggested, is undergoing a process of problematization, because, in brief, it does not conform to the 'classical' biosecurity model. It has, in other words, destabilized previous ways of understanding the world, motivating a regulatory response that is intended to reestablish order in the face of uncertainty and change, thereby enabling synthetic biology to be governed.

On one level, this research underlines that the task of selecting and naming new 'risk objects' for regulatory attention is one that requires considerable work on the part of scientific and technical experts engaged in biosecurity policy. As Michael Power (2007, p. 25) argues: "Experts work hard to construct objects for attention, to make them a common-sense object for management purposes". In the case of synthetic biology, as I have discussed throughout this chapter, numerous questions exist about 'who' or 'what' should be regarded as 'dangerous' or 'of concern'. In turn, biosecurity experts, drawing on synthetic biologists' claims about their science and its potential, engage in a demanding process of selection that requires sorting,

naming, and prioritizing the diverse risk aspects of synthetic biology, so they may be assessed and managed. Given the interpretive flexibility of what 'synthetic biology' is, and who 'synthetic biologists' are, these experts are presented with considerable scope to select and name an expanding taxonomy of 'dangers' and 'concerns'. For some, the possibilities enabled by DNA synthesis technology are worrying; for others, the genetic information bound up with increased knowledge about molecular life and biological processes; and for many, it is the promise of a biology that is 'simple to engineer', inviting those previously excluded from 'institutional science' to take part in 'potentially dangerous' research. In each case, it is with a view to 'difference' – differences that suggest new ways of 'doing biology' and new ways of 'being a biologist' – and by way of 'marking out difference' – relying on the construction of categories and lists – that potential 'biosecurity risks' are conceived and produced. Notions of 'difference' and 'otherness', in this context, are conceived and mobilized in two distinct, yet related ways: on the one hand, suggesting vulnerabilities or gaps in biosecurity – a defensive practice premised upon keeping 'dangerous tools' out of 'dangerous hands' – and, on the other, serving as a technique for drawing distinctions and distinguishing between who should count as a 'dangerous person' and what should count as a 'dangerous thing'.

On another level, this research sheds light on the performative impact of labels. Risk selection is not only 'an activity', but also 'an act', with implications for how people and things are understood and represented as particular kinds of social problems. Labeling theory, as Hacking (2002, p. 103) suggests, "asserts that social reality is conditioned, stabilized or even created by the labels we apply to people, actions, and communities". Or, as Butler (1993, p. 8) observes: "The naming is at once the setting of a boundary, and also the repeated inculcation of a norm." Therefore, the assertions made by experts not only describe, but also produce particular realities. In the case of synthetic biology, to speak of the science and its practitioners as 'biosecurity problems' makes these problems real. On the one hand, biosecurity experts variously depict the diverse 'tools' associated with synthetic biology as 'dangerous' or 'of concern', ascribing their worries not only to the 'physical' equipment that characterizes synthetic biology, but also to the 'intangible'

knowledge bound up with genetic information, as well as the aims and methodologies that set out the scope and nature of the field. Taken together, these labels contribute to locating anxieties about bioterrorism not only in the instruments and engineering concepts deployed by synthetic biologists, but also in the minutia of molecular life, embedding notions of 'danger' and 'concern' in genomes and genes, 'genetic circuits' and 'modular parts'. On the other hand, experts apply labels to the people, or the 'hands', that are said to constitute the 'synthetic biology community', and, in particular, those working on the margins of the science, who are said to be empowered by the tools of synthetic biology. However, as Hacking (2002) observes, labelling a person poses ethical dilemmas beyond that of labelling a thing, as people are not passive agents, but rather interact with the names that are assigned to them, changing, and being changed by, the name itself. Therefore, although 'biohackers' have not been directly linked to 'bioterrorism' and 'weapons of mass destruction', their discursive pairing with these concerns nonetheless changes and aggravates perceptions of their community.

5. Risk assessment: 'Pragmatism at the limits of predictability'

5.1 Introduction

In the previous chapter, I argued that, for many scientific and technical experts, synthetic biology is perceived to be problematic because it promises to 'democratize' modern biology, enabling more people in less formal research settings to gain access to 'potentially dangerous' life science resources. This framing of synthetic biology, I argued, serves to define and constrain the scope of what can be expected of the science, as well as its diverse practitioners. Both, I suggest, are now entangled in a biosecurity debate that envisions advances in biotechnology as embodying an 'intrinsic' (McLeish and Nightingale 2007) 'dual-use potential' (NRC 2004) that is perceived to merit some sort of regulatory response. Yet, as a number of commentators have pointed out (for example, Check 2005; IRGC 2009), although many appear to agree there exists a synthetic biology 'biosecurity problem', there remains considerable uncertainty about the kinds of 'biosecurity solutions' that might enable this problem to be made amenable to practical intervention.

With this in mind, in the following chapters I turn my attention towards ongoing efforts aimed at implementing 'practical interventions' – in other words, 'biosecurity solutions' – in the context of synthetic biology. Specifically, I will examine how those engaged in shaping biosecurity policy options for synthetic biology go about imagining its risks with a view to preventing its deliberate misuse and ensuring continued progress in a promising scientific field. In pursuit of this overarching research aim, this chapter will focus on the concept of 'risk assessment', which I define as a calculative technique aimed at understanding or rendering visible possible future harms. In the following chapter, I will then focus on the concept of 'risk management', which I define as a family of ways of intervening or acting upon those harms with a view to their prevention (among other regulatory objectives). Taken together, I will argue, risk assessment and risk management play a decisively pragmatic role in the synthetic biology policy debate, underlying a *risk*

management process that seeks to render synthetic biology's risks amenable to thought and action, that is, amenable to risk-based government.

Although I make the conceptual distinction between 'risk assessment' ('understanding') and 'risk management' ('intervening'), I do not intend to suggest that these functions are neatly separable. On the contrary, even though regulatory debates typically characterize risk assessment as a 'scientific' activity and risk management as a 'political' activity (Jasanoff 1987, 1995), which can be neatly compartmentalized as sequential steps, they are in fact "closely intertwined in practice" (Majone 2010, p. 120). This is because the setting of "regulatory priorities" is an outcome informed by numerous "scientific, economic, and political judgements" that are themselves "not easily separable" (ibid.). Therefore, to say that risk assessment comes 'before' risk management is, for me, more a matter of convention than a matter of practice. In fact, as I will discuss in some detail, one might just as easily make the counterargument, that is, risk management objectives shape how risk assessments are conducted, effectively reversing the more familiar sequence of 'cause' and 'effect'. In the case of synthetic biology, as in other spheres of science and technology characterized by not only the possibility of significant 'risks' but also significant 'benefits', there exists considerable incentive to develop policies that move the science forward, motivating risk assessments that are (at least in part) tailored to enable this outcome (Tierney 1999). Thus, although I will broadly address risk assessment in this chapter and risk management in the next, I by no means attempt to enforce their strict separation analytically.

How, then, are synthetic biology's 'biosecurity risks' assessed? How are they 'calculated'? How are they brought under a framework of technical intervention and control? Moreover, who is responsible for conducting these assessments, and what are the assessments intended to enable? These are among the key questions that will serve as a guide for this chapter (as well as featuring in subsequent chapters). On one level, these might be described as 'technical' questions, concerned with risk assessment as a mode of measurement or calculation. Yet, on another level, they are decidedly 'social' questions, concerned with aspects of risk assessment that are often glossed over by the very experts who conduct them, including problematic

assumptions about 'risks' for which there exist little historical precedent and limited scientific evidence. By focusing on both the technical and the social aspects of risk assessment, I underline that, in the case of synthetic biology, as in other spheres of social life, risk assessments are the product of both technical and social interactions. That is, they rely not only on scientific knowledge and (more or less) systematic standards of measurement, but also on imagination and intuition, rules of thumb and even guesswork. What matters, at least from the perspective of those who design or conduct the assessment, is that the risk assessment 'works' – that is, that it provides a 'risk estimate' that is not only reasonably precise, but also 'practical', enabling biosecurity interventions that are both achievable in practice and amenable to fulfilling particular risk management objectives.

5.2 An introduction to risk assessment in the context of science policy

Before addressing how synthetic biology's 'biosecurity risks' are assessed, it is worthwhile to briefly consider "the role of science in regulatory proceedings, an area of decisionmaking that is often generically described as 'science policy'" (Jasanoff 1990, p. 6). More precisely, it is important to consider how 'risk assessment', "a classic 'trans-scientific' activity carried out by regulatory agencies" (ibid, p. 216), has historically been understood and represented in science policymaking processes. By drawing on this history, I suggest, one is able to better appreciate the technical and political constraints that shape the present debate on synthetic biology. In particular, I wish to make two observations. First, the statistical technique of 'quantitative risk assessment' has traditionally been conceived as the benchmark of 'rational' policymaking, and, while this technique continues to be favored (as a regulatory ideal, if nothing else), the possibility of 'objective' risk assessment is increasingly contested. In particular, there exists a growing awareness of the 'limits of prediction', made evident by uncertainties associated with assessing emerging technologies, as well as a growing awareness of the diversity of risk assessment techniques (both 'quantitative' and 'qualitative') that inform, and have always informed, risk assessment in practice. Indeed, the types of

risk assessment techniques that are favored; the types of evidence that are deemed valid, and who should be made accountable for demonstrating that this evidence is sufficient, are all normative questions, which are understood differently at different historical moments and in different social and political contexts. Second, the 'purpose' of risk assessment in the context of science policymaking has historically been, and remains, a fundamentally pragmatic one. That is, risk assessment is premised upon the belief that risks can be known with reasonable confidence and be made the subject of interventions that can be used to satisfy particular policy objectives, including, but not limited to, mitigating the 'likelihood' and 'impact' (the traditional metrics of 'quantitative risk assessment') of possible future harm. In the following, I shed light on both of these dimensions with reference to several documents that have influenced how science policymaking (in the US, in particular) is understood and represented, and that vividly depict the historical precedents that underpin current efforts to assess synthetic biology's 'biosecurity risks'.

By some accounts, science policymaking based on 'risk analysis' – combining risk assessment and risk management – can be traced to an article written by the American electrical engineer and nuclear energy expert, Chauncey Starr (Kates and Kasperson 1983; Power 2007). Entitled, 'Social Benefit versus Technological Risk', and published in the journal *Science* in 1969, this article outlined an approach to science policymaking that aimed to achieve an 'optimal' balance between 'social benefits' and 'social costs' based on a 'quantitative' risk calculus. Having a significant impact in its time, it inspired a series of national scientific symposia and workshops, each premised upon Starr's (ostensibly) 'technical' approach to science policymaking (Kates and Kasperson 1983). According to Starr:

> "If we understood quantitatively the causal relationships between specific technological developments and societal values, both positive and negative, we might deliberately guide and regulate technological developments so as to achieve maximum social benefit and minimum social cost." (1969, p. 1233)

Whether Starr's vision for 'risk analysis' as it relates to guiding the regulation of emerging technologies was the first of its kind, or whether it merely represented a contribution to an ongoing movement towards risk-based regulation in light of the

uncertain health and environmental effects posed by emerging technologies such as nuclear energy, is open to interpretation (Short 1984; Weingart 1999). What can be said, however, is that Starr's approach to risk analysis – seeking to quantitatively determine causal relationships with a view to directing the optimal allocation of scarce societal resources – continues to represent a benchmark and 'technical ideal' (Power 2007) for science policymakers. Today, as in 1969, there remains at least the presumption that the 'actual' risks posed by advances in science and technology can be determined and that an 'optimal' balance between 'social benefits' and 'social costs' can be 'objectively' achieved. What is more, it tends to be with a view to science – and above all the science of 'quantitative risk assessment', often defined as a statistical technique premised upon calculating 'the probability of an event occurring multiplied by the likely impact of that event were it to occur' (Bradbury 1989) – that the 'right' balance is perceived to be possible.

Despite the prominence of 'quantitative risk assessment', as a technical ideal, the possibility of 'objective' risk analysis and 'value-neutral' policymaking is (and always was) elusive in practice. This is because the future cannot be known with certainty. Thus, decisions about how to prepare for future events remain obscured from objective understanding, underlying the 'limits of prediction'. As the economic theorist Brian J. Loasby (1976, p. 2) expressed in *Choice, Complexity, and Ignorance*: "Choice within a complex system cannot be fully informed; neither can the study of a complex system from the outside … [p]artial ignorance is intrinsic to problems of choice". While this observation applies to decision-making in all spheres of social life, it is especially apparent in relation to science policy, a domain typically confronted with intractable uncertainties due to scientific unknowns that are poorly characterized or, quite possibly, not even recognized. Moreover, "uncertainties in regulation", Irwin et al. (1997, p. 20) observe, are not simply the product of "technical uncertainties which can be reduced by further investigation and rational discussion". They are also "the result of … indeterminacies and conflicts in the policy-process resulting from the differing perspectives, interests and rationalities of different groups involved in regulation" (ibid.). Consequently, while informed by predictive techniques (quantitative or qualitative, formal or informal), regulators

must ultimately make decisions about how to allocate 'scarce societal resources' based upon human judgment, incomplete information and contrasting (expert) opinions. As the science and technology scholars Stirling and Mayer (2001, p. 530) rightly argue in relation to the assessment of technological risk: "Even the most ostensibly 'technical' citadels of the analytic approach – the quantification of probabilities and the measurement of harm – remain fundamentally context dependent, subjective, and thence political in character".

Contestation over Starr's strictly 'quantitative' interpretation of risk analysis is not only reflected in academic critique, but also in changing attitudes toward what should count as a 'good' decision-making model. Specifically, over the last half-century, confidence in the quantitative model has been gradually eroded, as the limits of prediction have come to be increasingly acknowledged by decision-makers engaged in designing regulatory policy (OECD 2010). One affect this has had, at least in terms of how risk analysis is represented in the context of science policymaking (which is not the same as saying that risk analysis has necessarily changed in practice), is the more explicit inclusion of 'qualitative risk assessment' as a valid mode of understanding, and, with this, the recognition that scientific knowledge is not the only type of knowledge that informs risk management processes. In the US context, this shift – from a strictly 'quantitative' to a more (but by no means exclusively) 'qualitative' interpretation of risk analysis – is perhaps most clearly demonstrated by two influential guides on risk analysis published by the National Research Council (NRC 1983, 1996); each intended to improve the US government's science policymaking efforts. Taken together, these guides reflect two rather different interpretations of risk analysis in the context of science policymaking – an activity that is increasingly represented as not only including, but also benefiting from, a more diverse range of knowledge and knowledge-making practices.

5.2.1 The 'Red Book' risk analysis model

The first, the so-called 'Red Book', published in 1983, describes a risk management process premised upon strict adherence to the quantitative model, where risk

estimates are represented as the rational outcome of a step-by-step, unidirectional process that requires limited human judgment and no additional knowledge beyond that afforded by science. In Figure 1, this process is illustrated by three successive stages – 'research', 'risk assessment', and 'risk management' – where scientific evidence about risks is not only represented as attainable, but, indeed, as the *only* type of evidence that merits consideration in the risk management process. At the same time, scientists (and scientific expertise) are represented as the singular source of legitimate knowledge about risks, and are accountable for producing risk estimates that are, in turn, used as a basis for implementing federal policies. In relation to the health risks posed by exposure to chemical or biological agents, for example, the Red Book describes 'dose-response assessment' as the "process of estimating the incidence of a health effect under the various conditions of human exposure" (NRC 1983, p. 20) providing "a concise estimate of adverse effect in a given population" (ibid, p. 28). In turn, policymakers use this estimate (according to the model) to guide and to justify specific policy actions (ibid.).

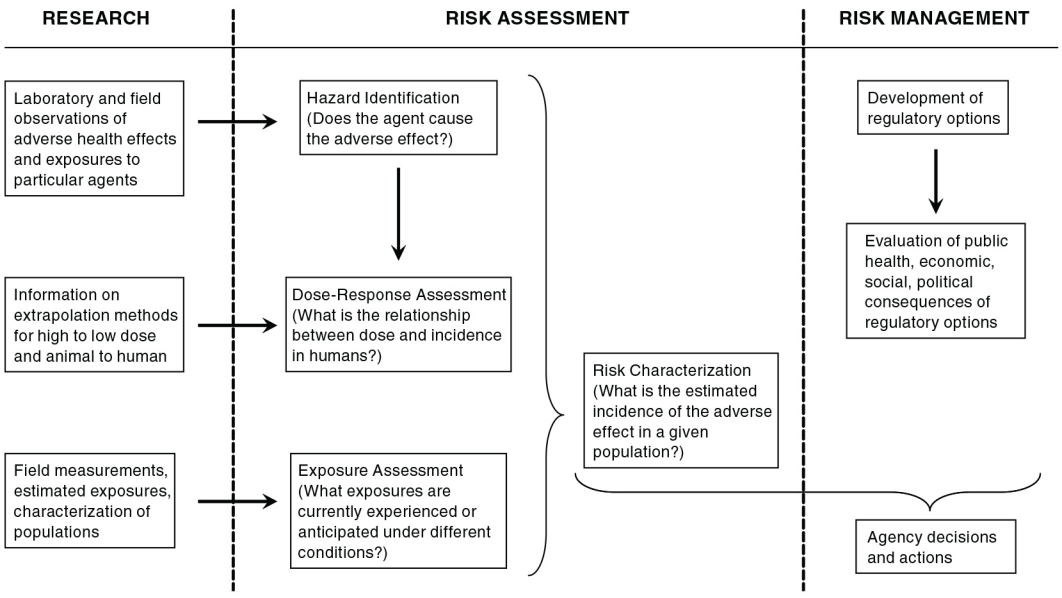

Figure 1: 'Red Book' risk analysis model (Source: NRC 1983, p. 31).

5.2.2 The 'Orange Book' risk analysis model

By 1996, with the publication of the so-called 'Orange Book' (the NRC's updated guide on risk analysis for science policymakers), this singular, science-based interpretation of risk analysis and its role in science policymaking was deemed to be out of date, and, moreover, not representative of how risk assessments are conducted in practice. Although observing that the Red Book's risk paradigm "remains prevalent in federal agencies"[74] (NRC 1996, p. 14), the NRC's views on risk analysis had shifted to the point of concluding that strict adherence to the quantitative model is "seriously deficient" (ibid, p. 16). The NRC cites several reasons for this, including: (1) the limitations of risk techniques that inform risk analysis; (2) fundamental uncertainty in information about risks; and (3) the fact that, despite claims to the contrary, risk analysis is a complex process that depends upon value-laden judgments and social deliberation (ibid.).

With this, the Orange Book proposes an alterative, "more robust" (ibid, p. 16), risk paradigm, described as an "analytic-deliberative process", where "[a]nalysis and deliberation can be thought of as two complementary approaches to gaining knowledge about the world, forming understandings on the basis of knowledge, and reaching agreement among people" (ibid, p. 3). In Figure 2, this process is illustrated as recursive, where knowledge gained through analysis and deliberation folds back on itself, contributing to new problem formulations, new modes of understanding, and ultimately new risk estimates that result from adapting the assumptions and constraints of the model itself. In this light, risk estimates are depicted as the outcome of both technical and social processes, drawing on both quantitative and qualitative modes of assessment. In other words, risk estimates are represented (at least in part) as political in nature, built upon negotiation and compromise between social actors, which is depicted as providing space for more than one 'right' answer, in addition to more than one 'best' way of 'calculating' risks. At the same time, scientists are no longer represented as the sole

[74] An observation, I will argue, that is equally valid today.

source of legitimate knowledge about risks, but as one among several primary stakeholders contributing to the risk management process. In particular, policy specialists are represented as playing an equally prominent role in risk assessment and risk management decisions (Wolt and Peterson 2000).

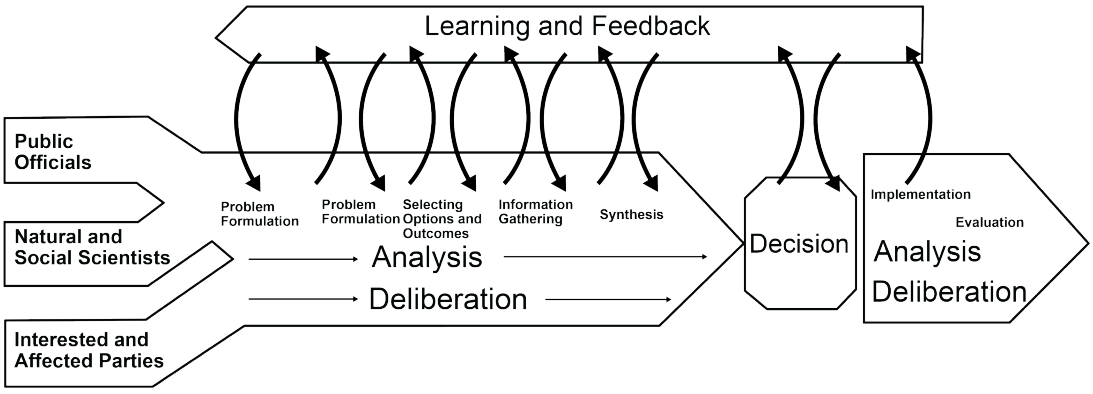

Figure 2: 'Orange Book' risk analysis model (Source: NRC 1996, p. 28).

Having highlighted what would appear to have changed with regard to how risk analysis is *represented* in science policymaking processes, I wish to highlight what I would suggest remains the same *in practice*. That is, despite endorsing different methods – the former calling for strict adherence to quantitative, science-based risk assessment techniques, and the latter more qualitative, social-analytic ones – both models (NRC 1983, 1996) are premised upon the assumption that methodologies exist that can be applied to the assessment of complex risk phenomena. Moreover, each methodology describes a more or less structured process that seeks to produce a risk estimate that can be used to inform and to justify practical objectives. "The purpose", the Orange Book suggests, "of risk characterization is to enhance practical understanding and to illuminate practical choices" (NRC 1996, p. 16). The term 'practical' merits emphasis. This is because science policymaking is inevitably characterized by "a mix of scientific and policy considerations" that blur the boundary between 'science' and 'politics' (Jasanoff 1987, p. 214). In other words, regulatory decisions are not simply the product of 'technical' procedures aimed at

deriving "a concise estimate of adverse effect" (NRC 1983, p. 20), but also the normative viewpoints and expectations of the scientists, public officials and policy specialists who inform the regulatory process with a view to 'optimal' policy outcomes. Thus, no matter how 'robust' the model, there remain numerous subjective considerations that inform the risk management process.

For this reason, 'pragmatism', I suggest, can be thought of as a unifying feature of both models (NRC 1983, 1996), and risk analysis more generally, especially when the potential rewards stemming from science and technology are deemed to be high. In such cases, the 'purpose' of risk analysis, at least from the perspective of regulators, is not only a risk estimate that is reasonably precise – representative of the 'actual' risks – but also 'practical' – enabling risk management actions that satisfy a variety of policy objectives, including aspirations for economic development and regulatory consistency. This 'goal-oriented' approach to regulation underlines, as Jasanoff (1993, p. 129) rightly argues, that the view that it is possible to separate "risk assessment (what we know about risk) from risk management (what we wish to do about risk) is one dogma that is clearly in need of profound and critical reexamination." Indeed, the determination to render risks visible so that they may be managed – in a variety of ways and with a view to a variety of policy goals – is a defining characteristic of regulatory activity that seeks to maximize the 'benefits' and minimize the 'risks' of science and technology. As Ewald (2002, p. 287) suggests, the very principle of 'sustainable development', which underpins science policymaking, "prohibits inaction in the face of uncertainty, at the same time that [it] seeks to limit as far as possible its harmful consequences." Thus, pragmatism, I suggest, even (or perhaps especially) at the 'limits of prediction', plays a central role in shaping risk estimates, as well as the 'quantitative' and 'qualitative' techniques that inform them. In the following section, I will argue that biosecurity risk assessment in the context of synthetic biology is an exemplary case of, what I refer to as, 'pragmatism at the limits of predictability'.

5.3 Biosecurity risk assessment in synthetic biology: In need of a 'new' standard?

Despite growing awareness within science policy circles that risk assessment does not conform to an absolute standard, and that 'value-neutral' policymaking is an ideal and not an empirical reality, there nonetheless remains a strong attachment to the scientific model (NRC 1983), which effectively remains the benchmark, and, indeed, the de facto 'standard' (Jasanoff 1987, 1990, 1993). In fact, in the US regulatory context, Jasanoff (1987, p. 197) has shown, "the legitimacy of American regulatory decisions uniquely depends on rational justification, in scientific as well as in economic and legal terms." In practice, Jasanoff suggests (ibid.), this means that policymakers and regulators, while often acknowledging that the 'risks' associated with advances in science and technology are characterized by irreducible uncertainty and that the policy process is informed by both 'scientific' and 'political' considerations, believe it is necessary to "present the public with a convincing scientific rationale for actions dealing with technological hazards, marshalling the supporting data and rejecting contrary evidence as persuasively as possible."

In the context of the life sciences, this conflicted stance is manifest in an ambivalent attitude towards biological risk assessment,[75] which, on the one hand, is judged to be a more or less subjective process, and, on the other, a more or less objective one. For example, this stance is clearly visible in relation to recent biosafety guidelines (CDC/NIH 2009), jointly issued by the US Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH), which provide guidance for life scientists on how to assess and manage biosafety and (more recently) biosecurity risks in the context of the laboratory. On page 16, the CDC/NIH guidelines state that: "Biological risk assessment is a subjective process

[75] 'Biological risk assessment', or 'biorisk assessment', is a term increasingly employed in guidance documents to describe risk assessments directed at assessing the 'likelihood' and 'consequences' of either 'biosafety risks' ("risks of accidental infection") or 'biosecurity risks' ("risks of unauthorized access, loss, theft, misuse, diversion or intentional release") (WHO 2006, p. iii). In this context, 'biosafety risk assessment' and 'biosecurity risk assessment' are understood as sub-sets of 'biorisk assessment'. See WHO (2006) for a more detailed discussion of this terminology.

requiring consideration of many hazardous characteristics of agents and procedures, with judgments based often on incomplete information. There is no standard approach for conducting a biological risk assessment". On page 107, that: "A biosecurity risk assessment should analyze the probability and consequences of loss, theft and potential misuse of pathogens and toxins." In other words, 'quantitative risk assessment' (at least its vocabulary and distinctive logics, if nothing else) remains central to notions of risk manageability; even when life science regulators are confronted with hazards that appear (by their own account) to cast doubt on its singular capacity to objectively 'calculate' potential harm.

A closer look at 'biosecurity risk assessment', as defined by the CDC/NIH, offers a more nuanced picture of how assessments of this kind are conducted in practice. Departing from the idealized model of biosecurity risk assessment as a more or less 'quantitative' procedure, relying on the analysis of 'probabilities' and 'consequences', this characterization of biosecurity risk assessment invites considerably more subjective leeway and imagination on the part of life scientists. Specifically, the CDC/NIH (ibid, p. 108) suggest that researchers should "[d]evelop a list of possible biosecurity scenarios" that take into account both the risk characteristics of a particular agent and the "motive, means, and opportunity of … potential adversaries ["Insiders" or "Outsiders"]" to acquire and misuse this agent. Based on these scenarios, researchers are further advised to "[e]valuate the probability of each scenario materializing (i.e., the likelihood) and its associated consequences" (ibid.). In other words, they are advised to conduct, first, a 'qualitative scenario analysis' – requiring imputations of potential 'agents' and 'adversaries' (including their 'motives') – with a view to possible biosecurity incidents, and, second, a 'quantitative risk assessment' aimed at evaluating the 'probability' and 'consequences' of potential bioterrorism attacks.

This 'mixed' risk assessment methodology, relying on 'quantitative' and 'qualitative' procedures, when contrasted with the strictly 'quantitative' biosecurity risk assessment model noted earlier (CDC/NIH 2009, p. 107), illustrates the apparent tensions that exist between biosecurity risk assessment in practice and idealized notions of biosecurity risk assessment as a more or less 'objective'

exercise. It also underlines that, although 'qualitative' judgments are deemed necessary in practice, 'quantitative risk assessment' persists as a technical ideal. It is precisely this faith in a scientific risk assessment standard, while acknowledging that such a standard does not exist, that creates a fundamental tension in science policy debates and regulatory processes. In the case of synthetic biology, this tension is visible in relation to frequently voiced concerns (see, for example, Bügl et al. 2007; NSABB 2010) about the 'appropriateness' of 'existing' risk assessment techniques in light of the potentially 'novel' risks engendered by the science. The argument being, 'novel risks fall outside existing modes of risk assessment and, in turn, fall outside existing regulatory frameworks'. As the National Science Advisory Board for Biosecurity (NSABB 2010, p. 32) describes this dilemma in relation to synthetic biology's biosecurity risks: "If it is believed that there are no new risks and that we can use an existing oversight structure, the situation would be very different from one in which new risks are apparent that will require new means of assessment and management." This argument, as I have suggested, is premised upon the assumption that there does indeed exist a 'standard' mode of risk assessment, one that has informed, and continues to inform, risk estimates in the context of the life sciences. Moreover, as the CDC/NIH (2009) suggests in relation to biosecurity risk assessment, it is assumed that this standard is a 'scientific' one.

In this section, I will argue that this assumption does not reflect risk assessment in practice, neither in relation to synthetic biology, nor in relation to previous iterations of biotechnology. Rather, there exist a variety of risk assessment techniques – quantitative and qualitative, formal and informal – that are used and adapted to assess and manage 'new' and 'emerging' risks. What this means, in practice, is that risk assessment techniques are not so much 'surpassed' or 'exceeded' by the emergence of a 'kind' of 'risk beyond measurement' or 'risk beyond risk' (Ewald 2002), but rather these techniques are continuously (re)invented to make 'new' risks 'fit' existing regulatory frameworks and specific risk management objectives. In the case of synthetic biology, as in the case of previous biotechnologies, while the 'risks' may at times be described as 'complex', even 'beyond assessment', they are nonetheless *currently* being assessed by an

assortment of techniques, which do not easily coalesce under a singular, preexisting risk management framework or risk assessment standard.

In the following, I will present my argument in two parts. First, I will argue that recombinant DNA technology, a precursor to synthetic biology, has previously been represented as both 'novel' and amenable to 'practical intervention', being made to 'fit' an existing regulatory framework and specific risk management objectives. Second, I will argue that synthetic biology is undergoing a similar process, raising familiar dilemmas, but also new ones. What is perceived to complicate risk assessment in relation to synthetic biology, I suggest, is not only reflected in the 'novelty' attributed to the science, but also in the 'new', or at least less familiar, context within which the science is embedded, namely, the contemporary context of biosecurity. When viewed in relation to 'biosecurity', having as its focus the problem of 'deliberate misuse', synthetic biology does not align easily with risk assessment techniques and regulatory frameworks that have been configured to address issues of 'biosafety', having as its focus the problem of 'unintended consequences' (Bügl et al. 2007). Thus, beyond any unique attributes that might be attributed to the science, synthetic biology presents regulators (and others who design and/or conduct biosecurity risk assessments) with a different set of challenges and priorities, calling for somewhat different 'standards' of assessment and management. In the following section, I will then examine one case of biosecurity risk assessment in more detail – specifically, the case of the US government's recently introduced 'screening methodology' for DNA synthesis providers (DHHS 2010b) – where these challenges are presently being negotiated, and risk assessments of this kind conceived and put into practice.

5.3.1 The Coordinated Framework for Regulation of Biotechnology: Pragmatism written into federal policy

Perceived 'challenges' to risk assessment in the life sciences, including those associated with scientific uncertainty and the limits of prediction, did not begin with synthetic biology. Rather, similar perceived challenges have accompanied a

succession of emerging biotechnologies – the most common reference technology in relation to synthetic biology being 'recombinant DNA technology' or 'genetic engineering'. Like synthetic biology, the potential risks posed by genetic engineering gained the attention of scientists and science policymakers at an early stage of the science's development. Beginning with the Asilomar Conference in 1975, questions were raised about the unknown – potentially unknowable – consequences of releasing genetically engineered (or 'recombinant') organisms into the environment. These concerns contributed to a scientist-led moratorium on certain kinds of genetic engineering experiments. Yet, this moratorium was temporary. Over the following decade, restrictions on genetic engineering experiments were gradually eased, with the exception of several categories of federally funded genetic engineering experiments that were deemed to require the NIH Director's approval on an individual basis (Office of Science Technology and Policy 1986).

In the mid-1980s, concerns about genetic engineering culminated with the drafting of the *Coordinated Framework for Regulation of Biotechnology* (hereafter referred to as 'the Framework') – a policy framework that continues to define US regulatory requirements for the application of biotechnology. A closer look at the Framework reveals how biotechnology has, since it inception, been perceived to pose 'novel' risks, yet has been made to 'fit' existing regulatory frameworks and specific risk management objectives. Understanding that this has been possible in the past (or at least 'possible' according to US regulatory standards), I suggest, is an important step towards demystifying synthetic biology, and the 'exceptional' status that is often ascribed to the science and its potentially 'incalculable' risks.

Drafted by the Office of Science and Technology Policy, and published in the Federal Register on 26 June 1986, the Framework builds upon the findings of an interagency working group assembled under the auspices of the (now former) White House Cabinet Council on Natural Resources and the Environment, which met in the spring of 1984.[76] The Framework addresses the regulatory requirements of

[76] Reminiscent of current regulatory efforts directed at synthetic biology, albeit with a view to 'safety' and not 'security': "The working group sought to achieve a balance between regulation adequate to ensure health and environmental safety while maintaining

the three primary federal agencies responsible for the oversight and regulation of biotechnology.[77] What is significant about the Framework is that it enabled genetically engineered organisms to be assessed and managed in a manner analogous to naturally occurring ones. In the context of environmental or agricultural applications of biotechnology, the Framework suggests:

> "[T]he means for assessing rDNA [recombinant DNA] organisms can be approached by analogy with the existing data base gained from the extensive use of traditionally modified [relying on selective breeding practices] organisms in agriculture and the environment generally. With step-by-step assessment during the research and development process, the potential risk to the environment of the applications of rDNA organisms should be minimized." (Office of Science Technology and Policy 1986, p. 20)

In other words, the Framework "reflected a position that biotechnology could be adequately regulated through the existing federal infrastructure and by adapting existing laws to new technologies" (Belson 2000, p. 269). The assumption being, 'there is nothing *inherently riskier* about organisms that are assembled using genetic engineering techniques than organisms that are taken from the natural environment and reconfigured to produce ordinary biological products' (NRC 1989). This meant that, for the purposes of oversight and regulation (including for the purposes of developing biological containment standards, export controls, and alike), a genetically engineered organism's risks could be assessed on the basis of the biological characteristics of the recipient (the organism that receives the DNA) and donor (the organism that donates the DNA) organisms alone; effectively making the recombinant organism *no riskier than the sum of its parts*.[78]

---

sufficient regulatory flexibility to avoid impeding the growth of an infant industry" (Office of Science Technology and Policy 1986, p. 4).

[77] That is, the US Department of Agriculture (USDA), the Environmental Protection Agency (EPA) and the Food and Drug Administration (FDA).

[78] In contrast, EU regulators drew a very different conclusion on the nature of the risks posed by recombinant organisms, which, in turn, contributed to a very different policy outcome. Specifically, in 1990, under Directive 90/220/EEC on the Release of Genetically Modified Organisms, the EU formalized a regulatory approach based on the 'precautionary principle', premised upon the belief that recombinant organisms could in

Equally significant were the 'exceptions'. According to the Framework: "The vast majority of industrial rDNA large-scale applications will use organisms of intrinsically low risk which warrant only minimal containment" (Office of Science Technology and Policy 1986, p. 20).[79] In other cases, further review, and possibly further biological containment, would be necessary. However, the authors of the Framework underline that 'knowing' what should count as an 'exception' is problematic: "Any proposal to regulate the research and products of genetic manipulation techniques quickly confronts the issue of what organisms should be considered appropriate for certain types of review" (ibid, p. 15). At the same time, despite the indeterminacies anticipated in determining which genetic manipulations should be categorized as especially risky, the Framework, *in no uncertain terms*, defines two such cases. The first refers to genetic engineering work that results in an "intergeneric organism" (ibid, p. 15). The second refers to genetic engineering work that involves a "pathogen" (ibid.). A closer look at each of these cases reveals that the reasoning used to interpret and define the exceptions as being 'exceptional' relied on considerably more than appeals to the 'scientific evidence'.

In the case of 'intergeneric organisms' (also referred to as 'new organisms', presumably because the recombinant product is deemed to be sufficiently different from either the donor or the recipient organism to merit this distinction), the exception is based upon the assumption that organisms of this kind (resulting from the combination of genetic material from two organisms from two different genera)[80] are likely to have a "*significant potential to exhibit new traits*" (ibid, p. 44,

---

fact prove to be *riskier than the sum of their parts*, thus meriting exceptional regulatory oversight and control. These contrasting assessments, which led to diverging policies, underscore the contingent character of science policymaking based on risk analysis. For a more detailed discussion on the subject of trans-Atlantic biotechnology policy and its divergence, see Lynch and Vogel (2001).

[79] The authors of the Framework draw this conclusion despite making the following aside on page 15: "This does not mean to suggest that the behavior of a genetically manipulated organism exempted from these definitions is wholly predictable (since any biological organism is never 100% predictable), but that the probability of any incremental hazard compared to the unmodified organism host is low."

[80] Biological classification based on Linnaean taxonomy groups species according to their shared physical characteristics. Species are ranked according to a hierarchical

emphasis in original), thus posing potentially novel risks. The exception is contrasted with 'intrageneric organisms' (genetic combinations from two organisms of the same genera) and is based upon the assumption that "intra-generic combinations" are "less likely to produce new combinations of traits than inter-generic combinations" (ibid, p. 45), thus posing no novel risks.

The rationale behind this distinction (that is, between the 'exception', *inter*generic organisms, and the 'non-exception', *intra*generic organisms) is not entirely clear. Why, for instance, base the distinction on 'genera' and not on some other taxonomic rank, such as 'species' or 'family'? For that matter, why not use some other metric entirely? Whatever the reasoning behind the choice, what can be said about this distinction is that it was not based on scientific evidence alone. If anything, given the following justification offered in the Framework, the choice appears to have been motivated by pragmatism, if not a sense of *practical necessity*. From the perspective of the Environmental Protection Agency (EPA): "[although] the Agency realizes that science provides no absolute standard for such distinctions", the "EPA believes the approach it has adopted is practical and facilitates the identification of those microorganisms that should be subject to special attention and also that should be considered 'new'" (ibid.). In other words, there was a perceived need, for the purposes of oversight and regulation, to definitively 'know' which recombinant organisms were 'riskier' than others. This, in turn, required that risk assessment techniques (in this case based on Linnaean taxonomy and the opinions of the EPA) be crafted to make this objective possible.

In the case of 'pathogens' – defined as a "microorganism that has the ability to cause disease in living organisms" (ibid, p. 43) – the reasoning is seemingly more straightforward. The exceptional status attributed to genetic engineering experiments that involve the use of pathogens is justified on the basis of the epidemiological characteristics of the donor and recipient organisms. In other words, 'pathogens are especially risky, therefore recombinant organisms derived from pathogens are also especially risky'. Moreover, according to the EPA,

---

classification system composed of seven ranks, from most inclusive to least inclusive: kingdom, phylum, class, order, family, genius, species.

"[p]athogens are a clearly defined category of organisms", which makes this category particularly practical for the purposes of regulation (ibid.). Yet, even this seemingly 'straightforward' claim – that pathogens represent a 'clearly defined category' – is not (or, at least, is no longer) self-evident. In the case of synthetic biology, as I will discuss in the following, there is no longer perceived to be anything 'clear' about a pathogen 'category' based on Linnaean taxonomy.

The Framework offers further cases of 'pragmatic policymaking', including several exceptions within the 'exceptions', which are said to reverse their exceptional status.[81] However, for the purposes of my argument, the cases that I have presented effectively underline my point. That is, previous biotechnologies (in this case, genetic engineering) have been perceived to pose 'novel' risks. These risks, in turn, have been made to 'fit' existing regulatory frameworks and specific risk management objectives. This can be seen in relation to an entire class of risk ('recombinant organisms') or in relation to the exceptions within this class ('intergeneric organisms' and 'pathogens'). In both cases, a combination of risk assessment techniques – some formal, others informal; some based on science, others on the perceived needs of the participating regulators – are brought to bear on problematic entities, and used to render them visible and manageable. In the case of synthetic biology, there are similarities to be drawn from past experience, and there are differences. Although not necessarily 'unique', the case of synthetic biology, I will argue, is nonetheless perceived to pose its own 'challenges', requiring its own 'standards' of assessment and management.

[81] In the case of intergeneric organisms, "excluded are organisms that have resulted from the addition of intergeneric materials that is well-characterized and contains only non-coding regulatory regions such as operators, promoters, origins of replication, terminators and ribosome binding regions" (Office of Science Technology and Policy 1986, p. 16). In the case of pathogens, "excepted are organisms belonging to a strain used for laboratory research or commercial purposes and generally recognized as non-pathogenic according to sources identified by a federal agency", as well as "genetically engineered organisms developed by transferring a well-characterized, non-coding regulatory region from a pathogenic donor to a non-pathogenic recipient" (ibid, p. 17).

5.3.2 Similar, but different: Keeping pace with 'novel' risks

Before proceeding with the case study on the DNA synthesis industry, it is worth taking a moment to consider how 'biosecurity risk assessment' in the context of synthetic biology contrasts with 'biosafety risk assessment' in the context of genetic engineering, and how these differences are perceived to complicate the regulatory strategy described in the Framework. Based on the interviews conducted for my research, as well as the scientific and technical readings conducted for this research, two sites of comparison (and, indeed, conflict) are especially apparent, one relating to perceptions of *how the science has changed*, and the other relating to perceptions of *how the context has changed*. With regard to the first theme, synthetic biology is perceived to complicate existing risk assessment techniques (notably, those defined in the Framework) that depend upon 'knowing' the risks based on the biological characteristics of 'naturally occurring' organisms. With regard to the second theme, the problem of risk assessment in synthetic biology is closely tied to the broader issue of 'deliberate misuse'. In both instances, what is deemed to be especially problematic about synthetic biology is that it does not 'match up' with familiar or established 'ways of knowing' the risks. Significantly, these tensions raise questions not only about *how synthetic biology's risks should be assessed*, but also about *who should be responsible for conducting the assessments*. Finding practical solutions to these challenges, in turn, is perceived to be central to enabling synthetic biology's risks to be made amenable to risk management or regulation.

First, for many scientific and technical experts seeking solutions to the problem of risk assessment in the context of synthetic biology, the possibility that the science might enable individuals to construct genetic sequences that do not exist in nature is deemed to be especially problematic. In their first report on synthetic biology, which addressed the regulatory challenges presented by DNA synthesis technology, the NSABB (2006, p. 8) cautioned that: "It is now feasible to produce synthetic genomes that encode novel and taxonomically unclassified agents", making it "difficult to make a taxonomic assignment" and thus difficult to conduct an assessment (ibid, p. 6). According to one biodefense scientist (Volker Beck)

interviewed for my research, this possibility does not just complicate the task of risk assessment in synthetic biology, but indeed makes it all but impossible:

> "There is one issue that is different, from my point of view. There is a gap now in the existing regulation … all the legislation on genetic engineering is focused on natural template DNA. But what we see DNA synthesis companies doing now is synthesizing more and more sequences without a natural template, and, at present, we have no legal approach to this because, in principal, without a natural template you can't do a risk assessment … without a template, where's the risk? … if you look from the point of view of how we've setup our legislation … Then I would say we have a gap in understanding the real risks associated with these kinds of materials." (Volker Beck)

This view of risk assessment, and its perceived limitations, clearly reflects the logic outlined in the Framework, which, as I have discussed, argues that a 'recombinant' (or, in this case, 'synthetic') organism's risks can be assessed, but only in relation to the naturally occurring organisms from which the DNA is derived. In 1984, the year the Framework was written, this effectively covered all cases, as it was assumed that all genetic templates were effectively 'natural', that is, 'found in nature'.

Another biodefense scientist (Richard Weller) interviewed for my research expressed similar misgivings about the uncertainties associated with synthetic organisms, but did not go so far as to say that these uncertainties may prevent risk assessment entirely, merely that relative to genetic engineering, which he described as a "mature science", the risks are less predictable:

> "I think there's a bit more predictability in recombinant DNA. … As the technology matured, I think what's happened in recombinant, is the predictability of outcomes have become, you know, pretty good. It's not totally infallible, but the predictability is pretty good. Synthetic biology, on the other hand, you truly have the ability, if I really understand the potential of the technology, to really create something that is totally *de novo*. … something that has literally never previously existed in the context of life on earth. … I think the predictability of outcomes, once you've got all that stuff together and it's truly novel— it's very uncertain, it's risky in my opinion." (Richard Weller)

These examples provide only a small sample of the arguments that I have found on the subject of the perceived challenges to risk assessment posed by genetically modified organisms derived from 'synthetic DNA' or 'non-natural templates' or 'sequences that do not exist in nature', and I will return to this subject in relation to the DNA synthesis industry case study in the following section. At this time, what I wish to emphasize is only that there is perceived to be a mismatch between where the science is today and where the existing standards of risk assessment and regulation are today. Whether risk assessments are made 'impossible' by synthetic biology, or merely 'less predictable', there is perceived to be a heightened level of uncertainty introduced by the science, complicating familiar 'ways of knowing' the risks. Moreover, much like the earlier case of genetic engineering, some believe that, "regulators may insist on developing new biosafety guidelines", albeit this time with a view to "synthetic microorganisms" that "lack a natural genetic pedigree" (Tucker and Zilinskas 2006, p. 33).

Although only a partial step towards 'new biosafety guidelines', at least one point of uncertainty has been addressed in the most recent *NIH Guidelines For Research Involving Recombinant DNA Molecules* (NIH 2011). Specifically, the *NIH Guidelines* now define "synthetic DNA segments" as equivalent to their "natural DNA counterpart" (ibid, p. 10). This more inclusive definition of "recombinant DNA molecules" (ibid.) effectively enables 'synthetic DNA', the formally 'non-biological' molecule composed of 'off-the-shelf' chemicals, to be treated as if it is 'natural DNA', the widely regarded informational molecule that encodes proteins and biological systems. According to the NSABB (2010, p. 9), this new definition enables "the current risk assessment framework described in the *NIH Guidelines* [to] be used to evaluate synthetically produced nucleic acids". While this may be – that is, by eliminating the 'synthetic DNA/natural DNA' distinction both entities can be treated as equivalent for the purposes of oversight and regulation – this (distinctly pragmatic) policy effort does not address the primary source of uncertainty and concern previously voiced by the NSABB (2006), as well as by those interviewed for my research. That is, it does not address how scientists and regulators might assess the risks posed by 'novel combinations of synthetic DNA', which might correspond

with 'biological properties that do not exist in nature'. In other words, as the NSABB (2006, pp. 14-15) underlined at the conclusion of their first report on synthetic biology, under the heading, "Next Steps in Addressing Biosecurity Issues:" "How can possible risks associated with the generation of novel organisms be addressed?"

Similar reconfigurations of existing guidelines and risk assessment standards, adapted to keep pace with heightened uncertainties about synthetic biology, are also being developed beyond the US. Much of this adaptation, as I have just discussed, concerns the (re)definition of synthetic biology (and/or its component parts). As Huib de Vriend (2006, p. 51), who has closely followed related developments in the European context, describes the importance of this ongoing regulatory activity: "The definition of risks related to synthetic biology and, consequently, the need for specific risk management measures, depends on the definition of synthetic biology." In other words, much depends upon whether synthetic biology is defined as something 'new' or as something 'similar' to existing biotechnologies, as this definition is used as a justification for how risk management efforts should proceed, and whether regulatory standards need to change.

As I have already explored in this chapter, and as I will examine in further detail in relation to the DNA synthesis industry case study in the following section, there is a tendency to adapt the names and attributes of new technologies to fit existing regulatory standards. Huib de Vriend's research in Europe would appear to lend further support to this observation, as evidenced by the following account, explored in an extensive report on synthetic biology, entitled, 'Early social reflections on the emerging field of synthetic biology':

> "According to the Forum Genforschung of the Swiss Academy of Sciences, synthetic biology is considered a new research field, which usually involves more genes and results in changes that are more radical than those resulting from genetic modification. In spite of this difference, with respect to safety, the Forum argues that synthetic biology is similar to gene technology and can be understood as a subdiscipline of the latter. From this rather inconsistent argumentation the Forum draws the conclusion that in general, the creation of synthetic organisms is no more risky than the introduction of new species into

> an ecosystem, dealing with natural pathogens or gene technology as practiced to date. Thus, the criteria that apply for the risk assessment of genetic modification also apply to synthetic biology." (de Vriend 2006, pp. 51-52)

Here, de Vriend argues that, in the case of the Forum Genforschung's deliberations on risk assessment as it relates to the release of synthetically derived organisms into the environment, synthetic biology is defined as both 'new' and 'similar' – new enough to constitute a "new research field", but similar enough to "gene technology" that it can be considered a "subdiscipline" (ibid.). This framing is then used to justify the Forum's claim: "the creation of synthetic organisms is no more risky than the introduction of new species into an ecosystem, dealing with natural pathogens or gene technology as practiced to date" (ibid.). In essence, this is a twenty-first century rendition of the argument put forward by the authors of the Framework: simply replace the word, 'recombinant' with the word, 'synthetic'.

Second, an equally important site of conflict in experts' accounts about synthetic biology and risk assessment does not concern the perceived 'novelty' of the science, but rather the perceived 'novelty' of the context within which the science is embedded. This conflict is again clearly discernable in relation to the risk assessment and regulatory standards developed in the Framework. The Framework, as I discussed above, was designed to address the unintended health and environmental risks that might arise from genetically engineered products. The Framework, in turn, has informed (among other control measures) biosafety protocols for the safe handling and storage of genetically modified organisms (CDC/NIH 1999, 2009). These protocols have become a routine aspect of institutional science and rely on researchers or institutional biosafety committees (IBCs) to conduct the necessary risk assessments, and, in turn, differentially control risky organisms (WHO 2006). According to these protocols (CDC/NIH 2009, p. 10), a biosafety risk assessment should address three aspects of the genetically modified agent (again, with a view to the "wild-type" from which the agent's DNA is derived), namely: "its capability to infect and cause disease in a susceptible human or animal

host, its virulence as measured by the severity of disease, and the availability of preventive measures and effective treatments for the disease".[82]

In contrast, the Framework says nothing about the subject of 'deliberate misuse', and, to date, a policy approach equivalent to the Framework does not exist on this subject (NRC 2004; Bügl et al. 2007; NSABB 2010).[83] At the same time, in 2009, the CDC/NIH, observing that, "[t]he events of September 11, 2001, and the anthrax attacks in October of that year re-shaped and changed, forever, the way we manage and conduct work in biological and clinical laboratories" (CDC/NIH 2009, p. iii), grafted on a biosecurity risk assessment provision (detailed at the outset of this section) to the existing biosafety protocols. As was the case with biosafety risk assessment, life scientists are again requested to conduct the assessment. However, in this instance, 'the assessment' no longer calls for only an appraisal of the biological characteristics of the (genetically modified) agent (which, as I have suggested, is already perceived to be complicated by the advent of synthetic biology), but also an evaluation of the likely identity and actions of the actor who might choose (or not choose) to acquire and deliberately misuse this agent. Specifically, the CDC/NIH (ibid, p. 108) suggests that researchers should assess the "motive, means, and opportunity of … potential adversaries ["Insiders" or "Outsiders"]" in an effort an effort to anticipate and, to the extent possible, prevent the theft and deliberate misuse of dangerous biological agents.

---

[82] I will return to this observation and its significance in the following section. Notably, in the case of arbitrary sequence information, DNA synthesis providers regularly conduct biosecurity risk assessments even though none of these three criteria (which provide the basis for biosafety risk assessments) can be anticipated.

[83] Although an equivalent framework that addresses the deliberate misuse of genetically modified organisms does not exist, the US government's Select Agent Program addresses the handling, storage and transfer of approximately 80 high-risk pathogens and toxins, prohibiting certain individuals from gaining access to these entities (NRC 2010). I will discuss the significance of the Select Agent Regulations in the next section of this chapter in relation to the DNA synthesis industry. Separate policy on 'dual-use research of concern' (DHHS 2012), which seeks to address the deliberate misuse of life science knowledge (identified as a further gap in life science regulation), has recently been released, which I will discuss in detail in the following chapter.

Beyond the problematic language the CDC/NIH uses to describe 'potential adversaries', even beyond the implicit assumption that the 'adversary' could be the individual researcher conducting the assessment ('Insiders'), requesting that life scientists conduct biosecurity risk assessments presents life scientists with a task that, according to some (including a number of synthetic biologists interviewed for my research), goes beyond their familiar areas of expertise. The argument being, assessing an individual's 'motives' is rather different than assessing a genetically modified agent's biological characteristics. While both may be equally difficult to evaluate, the one is perceived to fall more squarely within the domain of the behavioral sciences and law enforcement, and the other more squarely within the domain of the life sciences. As one prominent synthetic biologist (Rob Carlson) interviewed for my research put it: "if you are concerned about potential threats from people using biology or developing new technologies; developing new products, then you need to have access to that information", implying that such information is not readily accessible to life scientists. A number of non-life scientists (for example, Selgelid 2007, p. 41) share this opinion, arguing that, "the scientific community is systematically denied information that is absolutely essential to estimate security risks." Other life scientists, including those actively engaged in US biosecurity policy, emphasize that the very 'thinking' required to assess biosecurity risks is lacking among life scientists, as life scientists have traditionally been trained to anticipate and prevent 'laboratory accidents' and not 'bioterrorist threats'. According to David Relman, an infectious disease scientist at Stanford University and co-chair of the so-called 'Lemon-Relman Committee',[84] "'[researchers and IBCs] have not been adequately informed [about] how you think about biosecurity, how you think about the potential misuse of science'" (NRC 2007, p. 66).

This is not to say that synthetic biologists (or life scientists by any other name) dismiss the importance of biosecurity or the need for risk assessments that

[84] The Lemon-Relman Committee, also known as the 'Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats', was comprised of scientific and technical experts tasked with examining "current trends and future objectives of research in the life sciences that may enable the development of a new generation of future biological threats" (NRC 2006, p. VIII).

address the subject of 'deliberate misuse'. On the contrary, as discussed in the previous chapter, synthetic biologists (for example, LaVan and Marmon 2010) are at times exceptionally vocal about the potential 'biosecurity risks' engendered by their science and the need for greater education and awareness raising on the subject of biosecurity. For synthetic biologists, and for other stakeholders invested in synthetic biology's scientific and industrial development, attention to biosecurity is perceived to be essential for both mitigating the 'biosecurity risks' engendered by their work and sustaining the legitimacy of their science. In the words of LaVan and Marmon (ibid, p. 1012), synthetic biologists at the Massachusetts Institute of Technology, biosecurity is "vital for safe and effective progress within synthetic biology." But, it is to say that a common attitude, at least among the synthetic biologists interviewed for my research, is that life scientists can 'tell you about the science', but questions about 'motives' and 'intent', and about 'knowing' who is a 'potential advisory', are questions better left to law enforcement.

At the same time, experts specializing in aspects of national security, who ostensibly possess the necessary information (sometimes referred to as 'intelligence') to make an assessment of this kind, question the limits of their own knowledge. Specifically, they claim to lack information about 'the science'. As Christopher Park, a US counter-terrorism specialist, commented during an interview for my research: "At the end of the day, I'm not a scientist, so, to some extent, I'm limited by what information I've got." Or, as Piers Millett, a senior administrator for the Biological Weapons Convention, expressed: "Only the scientists and technologists know where the cutting edge is. And they only know because they're paid to follow it. We can't dabble and expect to understand." In both instances, although neither interviewee expressed that synthetic biologists "should identify the risks, or responses to those risks, on their own" (Piers Millet), they did express that addressing these risks will require their participation.

This view of shared responsibility, one in which life scientists are expected to actively participate in conducting biosecurity risk assessments and to engage with security experts on matters of 'national security', was particularly evident during an interview conducted with Special Agent You of the FBI's Weapons of Mass

Destruction Directorate. A key figure in the law enforcement community's outreach and awareness raising activities in synthetic biology, Agent You reasoned:

> "Who better to determine what the risks are than the people who are actually conducting the work? … For the FBI, if we've established the right dialogue, then the practitioners themselves can assist *us* in making sure we've allocated our resources to address the risk in a commensurate manner." (Edward You)

The question remains, is this a role synthetic biologists feel capable of fulfilling in the first place, and, if so, are they willing? While it may be desirable from the perspective of the FBI that synthetic biologists actively participate in conducting biosecurity risk assessments, and that researchers liaise with law enforcement agents on matters of 'national security', it may not be universally desirable from the standpoint of synthetic biologists. This mismatch in views represents a key site of tension that I will return to in Chapter 7 in relation to an emerging – albeit uneasy – 'partnership' between DIYbio and the FBI, one that is characteristic of recent efforts to establish a new 'culture of responsibility' in the life sciences, which increasingly favors a 'self-policing' scientific community.

Having highlighted some of the key tensions that characterize biosecurity risk assessment in the context of synthetic biology, as it relates to an earlier regulatory framework designed to address the unintended consequences associated with genetic engineering, I will now (in the second half of this chapter) explore an example of how these tensions are nonetheless being negotiated in an attempt to enable a 'secure' and 'sustainable' science. The case of the DNA synthesis industry, I will argue, much like the earlier case of genetic engineering described in the Framework, represents a case of 'pragmatic policymaking' – an approach to policymaking that is characterized by flexible modes of assessment (both quantitative and qualitative, formal and informal) that are designed and deployed to achieve a variety of policy objectives. While the science and the political and social context have changed since the advent of genetic engineering in the 1970s, the overriding motivation to develop science policies that are at once "accurate reflections of the world 'out there'" (Tierney 1999, p. 220) *and* conducive to 'practical interventions' remains much the same.

Before proceeding, I should underline that the case of the DNA synthesis industry represents only one site where biosecurity risk assessment standards are being developed. For example, as I have discussed already, biosecurity risk assessment has recently become a feature of institutional science, characterized by the introduction of risk assessment protocols that aim to anticipate and (to the extent possible) prevent the 'loss, theft and potential misuse' of biological materials (WHO 2006; CDC/NIH 2009). A further example, which I have not discussed in this chapter, relates to the role played by journal editors in the context of life science publishing, who have recently been called upon to identify, and, if deemed necessary, omit certain research findings that are classified as 'dual-use research of concern'. These examples (and others) represent the plurality of settings within which biosecurity risk assessment has become an integral component of risk management in the life sciences. In each case, while addressing the subject of 'deliberate misuse', the choice of risk assessment techniques and the manner in which these techniques are deployed, depend upon the specific risk management objectives they are intended to fulfill.

Thus, while I will examine the case of the DNA synthesis industry at this time, in the following two chapters I will examine in further detail how this plurality of sites of biosecurity risk assessment contributes to a family of ways of intervening that together constitute the risk regulation regime examined in my thesis. This said, as one of the most vigorous sites of biosecurity debate, the case of the DNA synthesis industry is illustrative of many of the challenges and dilemmas that confront life science regulators, life scientists, security officials, and others engaged in the problematic task of developing and/or implementing new biosecurity risk assessment standards and regulatory strategies in synthetic biology, making it a valuable site of empirical research in itself. Moreover, it provides a window into the particular 'mentalities of government' (ones that are, in this case, primarily 'managerial' or 'administrative' in function, directed at designing a structured risk management process) that are presently being harnessed to make a distinctly pragmatic objective – securing an emerging science while simultaneously ensuring scientific progress – possible.

5.4 'Know your sequence; know your customer': Biosecurity risk assessment in the context of the DNA synthesis industry

To date, few aspects of synthetic biology have received more policy attention than synthetic genomics. One of the so-called 'foundational technologies' (Endy 2005) that constitute the 'field' of synthetic biology, the capacity to direct the "construction of genetic material starting from information and raw chemicals" (Bügl et al. 2007, p. 627) has, in recent years, captivated the imaginations of science policymakers and regulators, motivating equal measures of enthusiasm and concern. The DNA synthesis industry, in turn, as the primary driver of this technology, has become a key site of policymaking activity. On the one hand, the economic success of this industry, which by some estimates generated between US$50-$80 million in 2008 (NRC 2010), lends support to synthetic biologists' claims that their science has the potential to yield significant economic benefits to governments that foster its industrial development. On the other hand, increased access to 'synthetic DNA', 'synthetic genes', and 'synthetic genomes', which DNA synthesis providers promise can reach customers within 48 hours "(from order to delivery)" (Bügl et al. 2007, p. 627), is perceived to be at odds with the competing political imperative of biosecurity. In fact, for some, the act of "keeping genes out of terrorists' hands" (Check 2009, p. 22) or "denying synthetic DNA to terrorists" (Maurer 2011, p. 1389) would appear to be indistinguishable from biosecurity itself.

In light of its perceived 'dual-use potential', a series of US government-sponsored initiatives have, in recent years, attempted to balance the 'potential benefits' of synthetic genomics against its 'potential risks', seeking to enable a 'secure' and 'sustainable' industry for synthetic DNA. Beginning with the NSABB's 2006 report, *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents*, which was informed by an *ad hoc* working group assembled by the NSABB, including consultations with "industry experts", "eminent researchers", "[US government] officials" representing multiple agencies and "key stakeholders" possessing relevant knowledge related to biosecurity and synthetic genomics (ibid,

p. 4), the tone of these initiatives has been one of apparent optimism. Specifically, participating experts have conveyed that, while synthetic genomics (and its application in the DNA synthesis industry) may present 'novel' biosecurity risks, these risks can nonetheless be understood and acted on with reasonable confidence. In other words, calculating risk estimates that can be used to inform and to justify risk management decisions in the context of the DNA synthesis industry, while at times described as "a prediction problem of the greatest complexity" (NRC 2010, p. 2), is perceived to be possible. Moreover, this belief has, I would suggest, never been in serious doubt. In contrast to statements made by the NSABB (2006) at the outset of their deliberations, the policy actions taken thus far would appear to reflect a policy approach based less on establishing if there is a need for an 'alternative' regulatory framework in light of potentially 'novel' risks and more on how these risks might be made to 'fit' a regulatory framework that already exists.

Published in its final form on 13 October 2010, the Department of Health and Human Services' (DHHS 2010b) *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA* (hereafter referred to as 'the Guidance') represents the culmination of the US government's recent policy efforts directed at the DNA synthesis industry. Building on the recommendations of the NSABB (2006), which called for a series of scientific and technical reviews on the part of the US government to address the 'biosecurity implications' of synthetic biology in general and synthetic genomics in particular, the Guidance is a response to the NSABB's call to establish, "strategies and mechanisms that might prevent or mitigate potential misuse of synthetic genomics while minimizing restrictions on the beneficial uses of this important field of science" (ibid, p. 3). In this section, I will examine how the Guidance – a governance 'strategy' or 'mechanism' intended to standardize biosecurity risk assessment practices across the DNA synthesis industry – attempts to fulfill this call, while simultaneously remaining within the boundaries of existing institutional and regulatory norms (in this instance, primarily the US Select Agent Regulations). Like the earlier Framework, the Guidance, I will argue, represents a case of 'pragmatic policymaking', one aimed at facilitating the assessment and management of 'novel' risks that exist at the 'limits of prediction'.

On the surface, the Guidance, much like the earlier Framework, might be described as a technical document that describes a disinterested approach to risk analysis based on appeals to the 'scientific evidence' (or, no less often, the lack of such evidence). In other words, it might be described in relation to the 'objective' or 'value-neutral' ideal embodied by the scientific model introduced at the outset of this chapter. However, beneath the surface, I suggest, the Guidance more accurately sets out to describe a more or less structured risk management procedure – combining an assortment of risk assessment techniques that have been selected and ordered as a singular 'strategy'. Characteristic of recent trends in regulatory decision-making, which ascribe to a 'procedural rationality' (OECD 2010, Annex 3.A1), this approach to risk assessment emphasizes 'transparency' and 'process' (in the absence of probability figures) as the basis for coherent risk policy (Power 2007; Bounds 2010). In this manner, to draw on Michael Power's (2007) conceptual understanding of risk management as an 'organizing practice', the Guidance is as much 'administrative' or 'managerial' in function as it is 'calculative' (in the narrow sense implied by 'quantitative risk assessment'). That is, it endeavors to establish a 'standardized formula' or 'blueprint' that can be used to organize uncertainty and enable choice and decision (ibid.). Although this is not to say that the 'risks' in question are strictly 'manageable', in the sense that this risk management effort or any other can necessarily prevent adverse events from happening, it is to say that these risks are treated *as if* they are possible to manage, "regardless of the extent of information about probability" (ibid, p. 6). In doing so, the Guidance offers one vision of how synthetic biology's biosecurity risks can be governed.

With a view to its functional or programmatic role as a visionary document, the Guidance can be understood as a regulatory instrument designed to manage "the risk assessment and management process" (Power 2007, p. 19). More precisely, it represents an approach to 'regulatory governance' (Wiener 2010) that operates by way of setting out instructions or guidelines for private companies to adhere to and to integrate into their daily business operations. In the words of Power (2004, p. 21), this approach to regulatory governance acts by way of "harnessing private control activities for public regulatory purposes", enabling regulatory organizations

to "be relieved of much of the economic and epistemic burden of detailed rule-making, and can oversee the design and functioning of local systems." Elsewhere, Power (2005, p. 591) has described this as, working "with the grain of industry practice, a theoretical win–win convergence of regulatory and economic capital." Sometimes referred to as 'management-based regulation' (Coglianese 2010), 'regulated self-regulation' (Power 2004) or 'enforced self-regulation' (Braithwaite 1982; Ayres and Braithwaite 1991), the underlying principle is one of governing 'at a distance' (Rose 2000), enabling regulatory agencies to act on risks indirectly by way of orienting risk management efforts and directing (in this instance) private companies to become responsible for managing the risks engendered by their work, and internalizing the costs of production (Power et al. 2009).

5.4.1 The 'screening methodology'

Referred to as the 'screening methodology' (DHHS 2010b),[85] the Guidance conceives of biosecurity risk assessment as encompassing two individual assessments, one addressing the risk aspects of the requested sequence and the other the risk aspects of the prospective customer. To briefly summarize this methodology, DNA synthesis providers are advised to conduct 'sequence screening' and 'customer screening' on an incoming order for synthetic double-stranded DNA. If either of these generates a 'red flag' or a 'hit', providers are then advised to conduct 'follow up screening' to ensure that the customer has a 'legitimate end-use' for the requested sequence. At this point, if there remain further concerns, the 'screener' – according to the Guidance, this is an in-house expert with the necessary expertise to "perform the sequence screenings, analyze the results and conduct the appropriate follow-up research to evaluate the significance of dubious sequence matches" (ibid, p. 21) – is advised to request the assistance of the FBI. In brief, as one expert interviewed for

[85] The terms and concepts in single inverted commas discussed in relation to the Guidance in this section are taken directly from various passages of the *Screening Framework* document (DHHS 2010b). In instances where I quote more lengthy excerpts from this document, I use double inverted commas, and cite the corresponding page number of the quoted material, as elsewhere in my thesis.

my research, who participated in the development of the Guidance, summarized the screening methodology: "know your sequence; know your customer".

Significantly, this shorthand – '*know your sequence; know your customer*' – is not only descriptive, providing a brief overview of the Guidance, but also, as I will discuss below, provides 'screeners' with a basic formula for conducting biosecurity risk assessments, where 'to know' is synonymous with 'to assess' and 'sequences' and 'customers' are synonymous with 'potential risks'. Although purporting to be a more or less 'objective' procedure devised to 'standardize' biosecurity risk assessment practices across the DNA synthesis industry, under closer examination the screening methodology proves to be a largely subjective (if practical) regulatory instrument. Before taking a closer look at both 'sequence screening' and 'customer screening', which effectively make risk assessment and risk management in the context of the DNA synthesis industry possible (again, 'possible' with respect to existing US laws and regulations), it is necessary to briefly discuss the US government's Select Agent Regulations, as these represent the de facto 'framework' within which DNA synthesis orders are (to a large extent) made to 'fit'.

Select Agents, as I have touched on already, comprise approximately 80 microorganisms and biological toxins that have been deemed by the DHHS and the USDA to pose a significant threat to public, animal or plant health.[86] Significantly, as I will discuss in relation to 'sequence screening' in the following, these biological entities correspond with a list of taxonomic names, and not the sequence information that describes individual pathogens. Equally significant, the designation of a Select Agent as being a 'Select Agent' is based on both biological and non-biological criteria, which means that not all pathogens (existing or potential) are included, even though they might ultimately pose a risk to public health. According to the 'Committee on Scientific Milestones for the Development of a Gene Sequence-Based Classification System for the Oversight of Select Agents' (hereafter referred to as 'the Committee on Scientific Milestones'),[87] the "designation of a microorganism

[86] See http://www.selectagents.gov/.

[87] This committee was the outcome of the NSABB's earlier recommendation to the US government to "convene a group of experts from the scientific community to conduct an

as a 'Select Agent' is a judgment call and a policy decision. 'Select Agent-ness' is not a strictly biological property" (NRC 2010, pp. 34-35). In other words, 'Select Agent' is a "regulatory term" (ibid, p. 35) and not a fixed property that is intrinsic to microorganisms. The Select Agent Regulations, in turn, seek to restrict "access to these microorganisms … and specify conditions under which legitimate research use may occur" (ibid, p. 36). These regulations also require the "registration of facilities including government agencies, universities, research institutions, and commercial entities that possess, use or transfer" Select Agents.[88] Finally, as the Select Agent Regulations are a US legal requirement, it should be emphasized that the Guidance, although "voluntary", is nonetheless intended to "remind providers of their obligations under existing regulations" (DHHS 2010b, p. 1).

5.4.1.1 'Know your sequence': Constructing 'controlled sequences'

Since the NSABB's 2006 report on synthetic genomics, and the potential risks arising from the DNA synthesis industry, the subject of 'sequence screening' has been a topic of particular 'dual-use concern' for regulators and DNA synthesis providers. The reason being, there is perceived to exist a regulatory (as well as legal) discrepancy between 'knowing the risks' associated with a predefined list of biological agents (which are covered under the Select Agent Regulations) and 'knowing the risks' associated with arbitrary sequence information submitted to a DNA synthesis provider (which may or may not encode a potentially dangerous biological agent, or part there of, and which is, in any case, not covered under the Select Agent Regulations). This discrepancy is perceived to be problematic from the perspective of both regulators and DNA synthesis providers, but for somewhat different reasons. For regulators, it is perceived to pose a problem of legal and regulatory consistency, as the Select Agent Regulations were never intended to address 'biological information', but rather 'biological agents', just as the

---

open and in-depth examination of the Select Agent classification system to determine if it is possible to reconcile the current controls for Select Agents with the anticipated scientific advances enabled by synthetic genomics" (NSABB 2006, p. 13).

[88] See http://www.selectagents.gov/.

Framework was never intended to address 'non-natural templates', but rather 'DNA that exists in nature'. For DNA synthesis providers, in contrast, it is perceived to pose a business risk and a liability problem. As one senior biodefense scientist expressed during an interview conducted for my research: "DNA synthesis providers are very aware that they are dealing with risky materials, and it is in their interest to not be accused in public that they are doing things beyond rational control." Or, as Christopher Park, who contributed to the development of the Guidance in his capacity as Senior Advisor for Bioterrorism in the Bureau of International Security and Nonproliferation at the US Department of State, argued: "DNA synthesis providers have a name to protect, and, more importantly, insurance premiums to pay" and therefore are "always going to exercise discretion about who they sell what to." This requires, of course, that DNA synthesis providers first know *what* they are selling – an objective that is complicated by the indeterminacies associated with arbitrary sequence information and differences of opinion on what should count as a 'controlled pathogen', and, in turn, a 'controlled sequence'.

In this light, there exist clear incentives for both regulators and DNA synthesis providers to develop an unambiguous definition of what should count as a 'dangerous', and, depending on the identity of the customer placing the order, 'prohibited' sequence. How these parties have arrived at a solution to this problem, however, has surprised many onlookers. This is because, the Guidance, as I will discuss momentarily, endorses a sequence screening standard that, by many accounts, is less rigorous than the industry sequence screening standards already adopted by many DNA synthesis providers. For some of the strongest critics of the Guidance, this suggests that regulators have opted in favor of regulatory 'convenience' and the perceived needs of industry over 'biosecurity' (Ledford 2010; Maurer 2011). While the extent to which these claims are justified is speculative, a closer look at the sequence screening standard endorsed by the Guidance reveals that, irrespective of the reasoning behind this particular approach to screening sequences, there do exist tradeoffs between 'practicality' and 'comprehensiveness' at the level of this (or any other) regulatory instrument's design.

According to the Guidance**,** DNA synthesis providers should screen orders against sequences 'unique to Select Agents' (referred to as 'sequences of concern'). Although the Guidance adds that providers are welcome to screen against further sequences, this is not a formal recommendation. DNA synthesis providers are further encouraged to use automated sequence screening software capable of identifying when a sequence more closely resembles a 'sequence of concern' (thus registering a 'hit') over any other 'benign sequence' (DHHS 2010b). "In this approach," which the Guidance refers to as 'Best Match', "the query sequence is aligned with a database of known sequences (such as GenBank) to identify the sequence with the greatest percent identity … over each 200 bp [base-pair] nucleic acid segment and corresponding amino acid sequence (or over the entire query sequence for those dsDNA [double-stranded DNA] orders shorter than 200 bps)" (DHHS 2010b, p. 11). These recommendations – the first relating to sequence screening based on a predefined list of Select Agents and the second relating to the use of automated screening software that employs the 'Best Match' technique – are justified in the Guidance on the basis of the following ('scientific') arguments.

First, the Guidance's exclusive focus on Select Agents is largely justified on the basis of the findings of the Committee on Scientific Milestones, which had previously concluded that, while it may be possible to augment the Select Agent List to accommodate the "sequence-based classification" of Select Agents (permitting them to be screened), it is not currently feasible to develop an "oversight system that predicts if a DNA sequence would result in an organism that should be regulated as a Select Agent" (preventing them from being screened) (NRC 2010, pp. 1-2). In other words, 'due to difficulties in predicting biological properties (for example, pathogenicity or virulence) on the basis of arbitrary sequence information, it is reasonable to focus only on those biological entities that are already known to be of particular concern, namely, Select Agents'. In effect, what this means is that all non-Select Agents (existing or potential) are beyond the scope of the Guidance's sequence screening standard (Maurer 2011). Although this argument, which is used to justify screening against only Select Agents, on one level, captures an important

empirical observation (one that has relevance not only to the case of the DNA synthesis industry, but also to the wider project of synthetic biology), namely, complex biological systems are not easily correlated with sequence information alone, it is, on another level, misleading; and for at least two reasons.

In the first instance, it is misleading because it assumes that unfamiliar sequences (which will be expressed as synthetic DNA if the order is processed) are benign, or at least they can be treated *as if* they are benign for the purposes of enabling the DNA synthesis industry to operate in the face of intractable uncertainty, even though the sequence might ultimately pose a risk. This biosecurity guideline, as it relates to the earlier biosafety guidelines established for recombinant organisms, is puzzling. This is because, in the case of recombinant organisms, as noted earlier in this chapter, knowing an agent's "capability to infect and cause disease in a susceptible human or animal host, its virulence as measured by the severity of disease, and the availability of preventive measures and effective treatments for the disease" (NIH 2009, p. 10) are the key criteria for conducting the risk assessment. Moreover, in the absence of knowledge about these properties (which is precisely the case when a DNA synthesis provider is confronted with an unfamiliar sequence order), the biological agent is assumed to be dangerous until proven otherwise. "Typically if we get an unknown agent," one biodefense scientist (Richard Weller) explained during an interview, "the standard global strategy is to handle it at the highest containment level possible until you decide it can be moved from a four to a three to a two.[89] But, where do you begin with a novel organism?" In the case of the Guidance, in contrast to the earlier biosafety guidelines, the corresponding unknowns are glossed over and the order is treated as 'safe' until proven 'dangerous'. In other words, unfamiliar sequences can be overlooked *on account of the limits of prediction*, and not the other way around.

In the second instance, it is misleading for reasons that are apparent on the very basis of the Select Agent Regulations introduced above. That is, the Select Agent

[89] Biosafety levels (BSL-1 through 4) "are designated in ascending order, by degree of protection provided to personnel, the environment, and the community" (http://www.cdc.gov/biosafety/publications/bmbl5/bmbl5_sect_iv.pdf).

List omits not only *unknown* pathogens (for obvious reasons), but also a variety of *known* pathogens, which are not included because they do not meet certain 'non-biological' and 'non-quantifiable' criteria for inclusion. For instance, the reason a number of Select Agents are on the Select Agent List is not because they are necessarily especially pathogenic, but because they have been used historically in biological weapons programs, for reasons such as their capacity to be transformed into environmentally stable aerosols that can be disseminated over large areas (for example, anthrax, a hardy spore-forming bacteria that can withstand prolonged exposure to harsh environmental conditions).[90] In contrast, the HIV virus, although unquestionably a dangerous biological agent, is not a 'Select Agent'. According to the infectious disease scientists, Casadevall and Pirofski (2004, p. 260), this is due, in part, to "the difficulty in delivering this virus to a susceptible host and because the disease occurs many years after the initial infection." In other words, it is not a Select Agent because it is not perceived to be a 'suitable' weapon.

There are further non-biological, non-quantifiable criteria beyond a Select Agent's weapons potential that are also used to justify a pathogen's inclusion (or non-inclusion) on the Select Agent List. In table 1, the Committee on Scientific Milestones outlines several criteria of this kind, which the DHHS and the USDA use to inform their decisions on what should count as a 'Select Agent' (NRC 2010). Here, the criteria are intended to demonstrate that even if the biological properties (such as pathogenicity or transmissibility) of an *unknown* pathogen could 'maybe someday' be predicted on the basis of its sequence information (which, as I have said, they conclude is presently not feasible), it could still not be classified as a 'Select Agent', as there remain non-biological properties (such as 'public perception' and 'natural prevalence') that can 'never' be predicted on the basis of sequence

[90] For a more detailed analysis on this point, see Casadevall and Pirofski's (2004) article, 'The weapon potential of a microbe', which argues that, "from a microbiological vantage point, there is no common denominator that ties the microbes on the select agent list together on the basis of their virulence or pathogenicity" (ibid, p. 260). Instead, "the weapon potential of a microbe", including its capacity to cause "terror if introduced into certain populations", appears to be the primary "consideration when categorizing certain agents as biological weapons" (ibid, p. 259).

information alone. This logic is then used to justify screening against only existing Select Agents, as these are the only biological agents that have been chosen on the basis of both their biological and non-biological properties. What is curious about this argument, however, is that it does not acknowledge, as I have said, that there exist many *known* pathogens, which could be Select Agents on account of their capacity to harm humans, animals or plants, but that are consciously excluded from the 'Select Agent List' on the basis of the very same non-biological, non-quantifiable criteria that effectively exclude unknown pathogens.

Table 1: "Prospects for *de Novo* Prediction of 'Select Agent-ness' from Sequence" (Source: NRC 2010, p. 34).

Property	Predictable Now?	Foreseeable Future?	Maybe Someday?	Never
Pathogenicity			X	
Transmissibility			X	
Available treatments			X	
Ease of preparation			X	
Ease of dissemination			X	
Public perception				X
Historical bioweapon				X
Economic impact				X
Natural prevalence				X

Although it does not appear to have been the Committee on Scientific Milestones' intention to draw attention to a gap or deficiency in the Select Agent Regulations, their logic effectively undermines the comprehensiveness of the Select Agent List; and thus its utility as the singular basis for sequence screening. In brief, it draws attention to the fact that the Select Agent List is incomplete, and not just because *unknown* pathogens are (unavoidably) not included, but because *known* ones are (consciously) not.[91] As several commentators (for example, Fischer and Maurer

[91] See McLeish and Nightingale (2007) for a similar discussion on the perceived limitations of agent-specific lists developed in the UK context. According to the authors: "in interviews several leading UK virologists expressed concern that some pathogens they regarded as being particularly 'dangerous' were not on the control lists developed by

2010; Maurer 2011) have pointed out, the Guidance also acknowledges that the Select Agent List (and, thus, the list of 'controlled sequences') is incomplete, but the subject is not pursued further within its pages: "The US Government recognizes that there are concerns that synthetic dsDNA sequences not unique to Select Agents or Toxins … may also pose a biosecurity concern" (DHHS 2010b, p. 9). In this light, although the Guidance may be 'consistent' with the existing Select Agent List (when updated to reflect sequence information in addition to a list of taxonomic names), and thus the Select Agent Regulations, it consciously ignores other pathogens that are known (unknown pathogens cannot be addressed in the Guidance or in any other screening framework), but that are not designated 'Select Agents'. This raises doubts about the 'scientific' rationality of the Guidance.

In contrast to the sequence screening standard set by the Guidance, two sets of industry standards, agreed first by the International Association Synthetic Biology (IASB) and later matched by the International Gene Synthesis Consortium (IGSC),[92] call for an approach to sequence screening that is not limited to Select Agents, but rather includes all known pathogens for which there exist sequence information in the GenBank database or equivalent sequence library. According to *The IASB Code of Conduct for Best Practices in Gene Synthesis*: "DNA sequences submitted as inquiries or orders for DNA synthesis by customers will be screened against GENBANK for reasonable sequence similarity to pathogens" (IASB 2009, p. 6). According to the IGSC's *Harmonized Screening Protocol*, DNA synthesis providers should "screen the complete DNA sequence of every synthetic gene order ... against all entries found in one or more of the internationally coordinated sequence reference databanks (i.e., NCBI/GenBank, EBI/EMBL, or DDBJ)" (IGSC 2009, p. 1).

Note that neither private sequence screening standard suggests that companies should screen against a universe of *unknown*, potentially dangerous sequences, as they, like the authors of the Guidance and like the Committee on

---

the UK government, whilst others they considered as not being particularly dangerous given the UK's climate were included" (ibid, p. 1646).

[92] See Fischer and Maurer (2010) for a more detailed account of how these two sets of industry standards came to pass, and how they eventually converged on the IASB's more 'rigorous' standard, despite early resistance from members of the larger IGSC.

Scientific Milestones that informed the Guidance, believe that this level of prediction is currently not feasible. What they do suggest, however, is that companies should screen against all *known* pathogens, irrespective of how they have been classified. Moreover, the IASB (2009, p. 6) goes one step further, suggesting that, in the event that screening technologies improve and are "empirically shown to detect threat sequences at reliability levels that meet or exceed the benchmark methods" used today, members will consider expanding the scope of their sequence screening assessments to include previously unscreened sequences.

For onlookers who have closely followed both the private and the public standard-making process, and who have expressed the opinion that the US government should endorse a more rigorous sequence screening standard than those already agreed by industry, "it seems strange for government to tell companies that current screening programs are, in effect, too ambitious" (Fischer and Maurer 2010, p. 21). According to Amy Smithson, a US-based chemical and biological weapons expert interviewed for my research who has closely followed these regulatory developments, she is "mystified" by the fact that the US government has opted to encourage the "lower standard":

> "Instead of requiring a screening procedure that required that *anything* that goes out the door does not have dangerous potential, they articulated the lower standard of, 'let's screen against the list of Select Agents'. And, from the get go, I have been mystified … It's just something to hang your hat on: 'Here, we will be secure if these "x" number of pathogens are restricted'. … you know, why focus on these, just because it's been done in the past?" (Amy Smithson)

Elsewhere Smithson (2010, p. 124) has similarly argued that the Guidance represents a "watered down approach that does not stipulate investigation of the potential dangers of orders for pathogens or DNA fragments beyond screening for whether they are on government high-risk lists."

However, from the perspective of at least one contributor to the development of the Guidance, Dana Perkins, a public health official and biological weapons expert working for the DHHS, the decision to screen against only Select Agents (and not all known pathogens) was simply intended to "keep a balance between risks and

benefits or between oversight and impeding progress", while holding the belief that the Select Agent List would provide an adequate starting point for the US government's involvement in the oversight and regulation of the DNA synthesis industry. According to Perkins, when developing the Guidance, the government sought "the minimum threshold of security":

> "Our view was that we have to start somewhere. So we started with Select Agents … we just wanted to give [DNA synthesis providers] the minimum threshold of security. So, some companies may still decide to go with higher levels of screening, but for those who were not doing anything, we're just giving them some guidance on how to start evaluating their business." (Dana Perkins)

Based on this account, which does not necessarily represent all those who participated in the development of the Guidance, it would seem that, 'a minimum threshold of security' was perceived to be desirable from a regulatory standpoint, but 'burdening industry' or 'impeding progress' was not.

Irrespective of which side of the debate one looks, what can be said about the decision to link the sequence screening methodology to the existing Select Agent List, is that it enables biosecurity risk assessment practices in the DNA synthesis industry to remain closely in line with the Select Agent Regulations. Moreover, in doing so, although the Guidance certainly simplifies the problem of sequence screening, in as much as it enables DNA synthesis providers to screen against a finite number of known pathogens documented on preexisting lists, it ignores a variety of potentially dangerous pathogens that could be (but are not) on those lists. Beyond the more speculative claims made by some of the most outspoken critics of the Guidance, who suggest government authorities have chosen to enable industry at the expense of security, the more subtle critiques argue that, while regulatory consistency and business efficiency may be worthwhile objectives, by "pruning the threat definition" – focusing exclusively on Select Agents – "this approach makes the problem *too* manageable" (Maurer 2011, p. 1424).

Second, by adopting an approach to sequence screening based on a predefined list of Select Agents, the Guidance simultaneously endeavors to enable DNA synthesis providers to use automated screening software[93] to screen against 'sequences unique to Select Agents'. According to the Guidance, their 'Best Match' approach to sequence screening, which is said to require "appropriate sequence screening software" based on a "publicly available suite of algorithms" such as "the BLAST family of tools",[94] will permit DNA synthesis providers to more or less unproblematically identify when a query sequence more closely resembles a 'sequence of concern' over any other 'benign sequence', thus registering as a 'hit' (DHHS 2010b, p. 20). In advocating for this approach to biosecurity, the Guidance once again appeals to the need for consistency, arguing that the use of sequence screening software will enable risk judgments to remain uniform and replicable across the DNA synthesis industry (DHHS 2010b). In other words, "a hit for one company should register as a hit for other companies adhering to the guidance."[95] In contrast, human screening, although not deemed irrelevant, is marginalized as being 'inconsistent'. The rationale being that human screeners are prone to disagree and often arrive at different conclusions based on the same data (Maurer 2011).

Critics of the Guidance, however, point to several gaps in this logic, each of which pertains to the notion of 'consistency'. On the most basic level, it is argued that, "consistency is not accuracy. Indeed," as Stephen M. Maurer, an Associate Professor of Public Policy at Berkeley University who has been among the strongest critics of the Guidance, argues, "a system could have a 100% error rate and still be consistent, provided it made the same mistakes every time" (Maurer 2011, p. 1423).

---

[93] For example, 'BlackWatch', a software package that aims to help DNA synthesis providers "screen all client sequences for matches to the sequences of hazardous pathogens" in an effort to identify "sequences worthy of concern" (http://biotech.craic.com/blackwatch/BlackWatch_Datasheet.pdf).

[94] BLAST refers to 'Basic Local Alignment Search Tool', and is used to describe a range of software tools used in bioinformatics to compare query sequences against sequence libraries in an effort to identify sequences that resemble the query sequence.

[95] 'Frequently Asked Questions: Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA' (DHHS 2010c), available at: http://www.phe.gov/Preparedness/legal/guidance/syndna/Pages/faqs.aspx.

Moreover, as I have underlined already, given that the Guidance recommends that DNA synthesis providers only screen against Select Agents, even if the software were perfectly accurate, it would still systemically overlook those sequences unique to pathogens that are not defined as 'Select Agents'.

The argument for consistency is also challenged on the grounds that neither the Guidance nor the Select Agent Regulations are free of subjective judgments, arbitrary cutoffs, and similar human 'inconsistencies'. In the case of the Guidance, as several commentators have pointed out, one should recall that the very decision to screen against 'synthetic double-stranded DNA', and not 'single-stranded DNA' or 'oligonucleotides' or any other possible candidate for screening, was a subjective choice. Moreover, by some accounts, including a recent news feature in the journal *Nature*, this decision has "drastically restricted the Guidelines' reach" (Ledford 2010, p. 898). Similarly, in the case of the Select Agent Regulations, as I have discussed, the very composition of the Select Agent List is the product of a range of non-biological, non-quantifiable (i.e. subjective) criteria that have been used to inform the choice of which pathogens get included and which do not.

Finally, perhaps the strongest case made against the need for consistency is simply that there is nothing necessarily 'wrong' with *in*consistency. For many critics of the Guidance, there is nothing 'deficient' about human screeners, nor their capacity to disagree and to draw different conclusions on the basis of the same data. On the contrary, human screeners are perceived to play a vital role in checking each sequence against the scientific literature, against GenBank, and against similar resources (interview with Amy Smithson), and are perceived to be more likely to pick up on anomalies that might otherwise be missed by the software (Maurer 2011). The purpose of these arguments, I would suggest, is not to dismiss the usefulness of screening software, but merely to underline that 'consistency' is not necessarily a virtue in itself, and even the most 'technical' modes of risk calculation are informed by 'subjective' human judgments, for better or worse.

Before taking a closer look at 'customer screening', I would like to consider one further aspect of the present discussion, namely, how might industry view the Guidance's proposed approach to automated sequence screening? As Maurer (2010,

p. 4) observes, from the perspective of DNA synthesis providers, one would expect that most providers would favor increased reliance on automated screening software directed at a finite list of Select Agents, as this would enable "expensive human screeners" to "be replaced by computers". In other words, it is "'fast' and 'cheap'" (ibid, p. 16). Yet, while this would make sense, in principle, as it might enable individual orders to be processed at a lower cost, there is nothing to suggest that DNA synthesis providers necessarily wish to screen less rigorously. On the contrary, as Maurer and other critics of the Guidance argue, industry's endorsement of screening all known pathogens (as opposed to only Select Agents) suggests precisely the opposite. That is, relatively 'rigorous' screening procedures seem to be of interest to many DNA synthesis providers. Thus, the Guidance's approach to sequence screening may not be precisely what industry desires.

To help clarify why this might be, and to help shed light on the irony that industry would appear to favor more intensive screening than government regulators, it is worthwhile to return to Christopher Park's comment introduced at the outset of the present discussion. That is, "DNA synthesis providers have a name to protect, and, more importantly, insurance premiums to pay". In other words, DNA synthesis providers are as concerned about their ultimate business liability (say, someone orders synthetic double-stranded DNA that is then used to produce a viable pathogen that is deployed in a bioterrorist attack) as they are their overhead on screening individual orders. Moreover, Schmidt and Giersch (2011, p. 9) argue, in opting for relatively 'rigorous' screening procedures, industry seeks to pre-empt potentially more restrictive "state-driven regulation" that could be implemented in the future. Therefore, ironically, and Maurer (2010) would certainly agree, while the DHHS may wish to push for 'the minimum threshold of security' in an effort to unburden industry, industry may very well wish for sequence screening to be 'less fast' and 'more expensive'; not the other way around.

5.4.1.2 'Know your customer': Constructing 'denied persons'

'Sequence screening' represents only the first half of the biosecurity risk assessment endorsed by the DHHS. According to the Guidance, 'sequence screening' should be accompanied, "in no particular order", by 'customer screening' (DHHS 2010b, p. 14). Yet, what is interesting (and, I would suggest, particularly revealing) about the 'screening methodology' is that the 'customer' component of the assessment is largely overshadowed by the 'sequence' component.[96] In fact, the 'customer', much like the generalized figure of the '(bio)terrorist' frequently evoked in (bio)security policy discussions, often appears to be absent from the risk calculation entirely, or simply characterized as a disembodied purveyor of potentially harmful sequence information. This gives the impression that the biosecurity risk assessment primarily (if not exclusively) concerns the sequence being ordered and the synthetic DNA it encodes, irrespective of how that DNA might be (mis)used.

Although there are multiple arguments that one might put forward as to why this is the case, one argument, I suggest, is that 'customers', as social actors imbued with human agency, are simply not as familiar to 'screeners' – individuals who are typically trained in bioinformatics and related scientific and technical fields (DHHS 2010b) – as 'genes' and 'genomes'. As discussed earlier in this chapter, there is perceived to exist a mismatch between 'knowing the risks' associated with 'unintended consequences' and 'knowing the risks' associated with 'deliberate misuse'. There are, in effect, two types of biological risk at play – one that relates to the biological 'things' in the laboratory, on the lab bench, and so on, and one that relates to the social actors who interact with those things and (mis)use them – each of which is perceived to benefit from somewhat different risk assessment techniques and different types of expertise. Thus, in the absence of secure knowledge about (unknown) 'customers', the Guidance favors (known) 'sequences'. Before proceeding with my discussion of 'customer screening', it is worth reflecting

[96] This is also true of critiques about the Guidance. That is, the dominant topic of discussion and debate in relation to the Guidance is 'sequence screening' and the challenges and dilemmas associated with defining and identifying 'sequences of concern'. To date, the topic of 'customer screening' has been relatively neglected.

on what it means to include a human agent in the risk calculation, and, equally, what it means to *exclude* a human agent from this calculation.

In light of the growing relevance of biosecurity risk assessment in the wake of 2001, the role of human agency as an integral component of 'biorisk' has become an increasingly salient subject at the level of federal policy in the US context. An excellent demonstration of this is a report prepared by the 'Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis' (hereafter referred to as 'the Committee on Methodological Improvements'). Published in 2008, this report critiques the methods used in the Department of Homeland Security's (DHS) annul Biological Threat Risk Assessment (BTRA),[97] offering advice to the DHS on how to improve their biosecurity risk assessment methodology. The "fundamental problem" with the BTRA, the Committee on Methodological Improvements argues, is that it treats "terrorist decision making exclusively as random variables, as is appropriate in the case of natural disasters" (NRC 2008, pp. 2-3). In other words, the Committee argues, the BTRA fails to account for the "behavior of an intelligent adversary", one that is "constantly adjusting tactics to exploit any evident weakness in US defenses" (ibid, p. 5). Politicized language aside, the point made by the Committee is rather clear: the DHS does not know how to model human agency for the purposes of the BTRA. Furthermore, in the absence of this capacity, it attempts to model social actors as if they are things (a 'natural disaster') and not persons (an 'intelligent adversary'). The Committee on Methodological Improvements' critique, I suggest, especially in light of the fact that it is directed at the DHS, a federal agency with considerable resources at its disposal, is a powerful demonstration of the uncertainties and methodological challenges perceived to be introduced by the subject of 'deliberate misuse'. It might also partly explain the relative absence of a human agent (or an

[97] Although the specifics of the BTRA are classified, the Committee on Methodological Improvements describes it as a "computer-based tool that has been applied by DHS to assess the risk associated with the intentional release of each of 28 biological threat agents categorized by the Centers for Disease Control and Prevention" (NRC 2008, p. 1).

'intelligent adversary') in the screening methodology, as well as in the broader debate on biosecurity in the context of synthetic biology.

In the absence of a reliable (or even a familiar) technique for assessing the risks associated with an 'intelligent adversary', the Guidance is rather vague on how screeners should go about 'knowing their customer'. According to the Guidance:

> "The purpose of *customer screening* is to establish the legitimacy of customers ordering synthetic dsDNA sequences. Providers should develop *customer screening* mechanisms to verify the legitimacy of a customer if the customer is an organization or confirm customer identity if the customer is an individual, to identify potential 'red flags'". (DHHS 2010b, p. 4)

In brief, the Guidance recommends that screeners verify the 'identity' of the customer, and, with this, make an assessment on their 'legitimacy'. Here, 'legitimacy' refers to a customer's legal right to gain access to Select Agents, as stipulated under the Select Agent Regulations. Beyond this minimal guidance, much of the responsibility for deciding how to verify a customer's identity and establish their legitimacy is the responsibility of the individual screener and the 'mechanisms' they develop. Government guidance of this kind – setting out the basic parameters for conducting assessments, but no more – is indicative of regulatory strategies aimed at managing "the risk assessment and management process" (Power 2007, p. 19), leaving much of the practical work of calculating risks and implementing risk management decisions to (in this instance) individual companies and their in-house experts. This mode of governance, sometimes referred to as 'management-based regulation', "leverages the private sector's knowledge about its particular circumstances and engages firms in developing their own internal procedures and monitoring practices that respond to risks" (Coglianese 2010, p. 160).

In practice, screeners draw on a set of 'indicators' (some of which are outlined in the Guidance; others communicated by interviewees who contributed to the development of the Guidance) that effectively serve as proxies for 'knowing their customer'. These include, requesting the "[p]rincipal user's full name and contact information"; their "[b]illing address and shipping address (if not the same)", and/or the "[p]rincipal user's institutional or corporate affiliation (if applicable)"

(DHHS 2010b, p. 13). These, according to Christopher Park, are essentially indicators adapted from the "export control world", which serve to provide screeners with a sense of "whether there is a reason to be concerned". Other indicators include, "the country of origin … the method of payment … types of letters of credit"; even the "type of letterhead" a customer uses to place an order. According to Park, although "nothing catches everything", institutional letterhead can at least provide screeners with a sense of whether or not the customer is affiliated with a "real facility". "Then there are the related questions," he explained:

> "Have you ever dealt with this customer before? If so, is this consistent with previous orders? Is it the same individual? Is it the same mailing address? Is it consistent with the kind of research you know is going on at the facility? If you have doubts, you call, you Google them … fairly straight forward stuff." (Christopher Park)

What this account suggests is that there is not a fixed approach to conducting customer screening. Rather, there exist a variety of questions screeners ask themselves, which serve to inform their risk judgments on which orders should be filled and which should not. According to Park, this risk assessment process is informed as much by intuition and experience as it is by objective 'facts' about the identity and motives of the customer in question. "At the end of the day," he explained, "you wind up having to plug in educated guesses (or whatever you want to call them), and that winds up being, to some extent, a gut thing." "It is also," he expressed, "reasonable to expect that companies will exercise a certain amount of common sense in terms of what they will send to a high school student who is working on a science fair project. But, to what extent, who knows?"

As a matter of legal accountability, DNA synthesis providers are also requested to check all incoming orders against a number of lists of 'denied persons', including the "Department of Treasury Office of Foreign Assets Control (OFAC) list of Specially Designated Nationals and Blocked Persons (SDN List)"; the "Department of State list of persons engaged in proliferation activities", and the "Department of Commerce Denied Persons List (DPL)" (DHHS 2010b, p. 15). For international orders, "most transactions involving Cuba, Iran, and Sudan are [also] prohibited"

(ibid, p. 16). Any customer who is found on one or more of these lists generates an immediate 'red flag' and their order is likely to be refused. For some experts, screening against lists of this kind (unlike lists of 'controlled sequences', a subject that has received considerably more attention) is perceived to be relatively unproblematic, falling into the "no brainer category". According to Amy Smithson, the problem with lists of 'denied persons' is primarily an administrative one:

> "Customer screening falls into the no brainer category. Governments already have lists of known middlemen, bad guys, criminals— There should be one point, one stop shopping, for the companies to submit that customer's name and other basic information, so that they can quickly screen through *all* the government lists. In the United States there's like 17 different agencies that have these lists. They shouldn't have to knock on 17 different government doors to get the screening done. It should be in one place." (Amy Smithson)

Similarly, Andrew Hessel, a prominent US-based synthetic biologist invited to speak at the BWC on the 'security implications' of synthetic biology during my field research, expressed that it is far more difficult to identify and screen 'dangerous sequences' than it is to identify and screen 'dangerous persons':

> "I think it's actually harder to screen for dangerous sequences, because we can take small elements— Put it this way, anything we think is a dangerous sequence, we could always break it down into smaller and smaller elements for assembly, and you can get past that filter. It's harder to get around your *identity*. … I think the key is identity – whether it's a corporate identity or an individual identity. Those are unambiguous." (Andrew Hessel)

In this account, unlike a sequence, which can be broken down into smaller and smaller parts to evade detection based on a predefined list of 'dangerous sequences', an individual's or an organization's identity is described as 'unambiguous', providing a more reliable metric for the purposes of screening.

Yet, for others, the process of 'customer screening' is anything but straightforward. Notably, during a workshop on the dual-use implications of

synthetic biology,[98] Mackenzie Cowell, co-founder of DIYbio, expressed his displeasure at the suggestion that DNA synthesis providers should not mail synthetic DNA to "P.O. Box addresses", a requirement that threatens to marginalize the research activities of 'non-institutional' biologists. Specifically, Cowell's concerns stem from the Guidance's recommendation that all customers not affiliated with an institution merit follow-up screening (DHHS 2010b), effectively excluding DIY-biologists from ordering synthetic DNA to advance their research projects.

In this light, it is apparent that, while the 'indicators' used by screeners to conduct their assessments serve to fulfill a specific objective – namely, as several interviewees expressed, they enable DNA synthesis providers to fulfill their "due diligence", thereby enabling orders to be filled in accordance with existing laws and regulations – they also threaten to exclude various ('non-dangerous') actors from gaining access to various ('non-dangerous') strands of synthetic DNA. The reason being, although indicators, as heuristic devices or simple rules of thumb, are practical, they also (necessarily) lack precision, and therefore cannot subtly differentiate between ('potentially dangerous') customers on a case-by-case basis. Moreover, lacking this level of precision, they threaten to exclude some individuals from participating in aspects of modern biology, and reify their status as 'risky subjects' or 'risks to society' – labels, as I discussed in the previous chapter, that are not without consequence for those to whom the label is applied.

Thus, in practice, in addition to explicitly including 'known middle men, bad guys and criminals', lists of 'denied persons' effectively include DIY-biologists, and for reasons other than their 'actual' motives and capabilities. As I argued in the previous chapter, DIY-biologists are perceived to be 'biosecurity problems' not so much because of what they might do with synthetic biology, but because of who they are and where they conduct their work – the Select Agent Regulations make no provisions for those working in their garage. Consequently, DIY-biologists occupy a liminal position, neither free to fully participate in synthetic biology nor explicitly

[98] 'Synthetic Biology and Nano-biotechnology Risk and Response Assessment Project', hosted by the United Nations Interregional Crime and Justice Research Institute, Turin, Italy, 24-25 March 2010.

forbidden from participating. Moreover, until the Select Agent Regulations are updated to reflect the growing trend in non-institutional biology – a trend that is at the core of the synthetic biology project, which aims to extend the tools of modern biology to more people in less formal research settings – DIY-biologists will continue to don a 'black hat', and, in the case of the screening methodology endorsed by the DHHS, elicit a 'red flag'. This said, although a troubling reality for DIY-biologists, this situation does not represent a coordinated or deliberate act of discrimination against their community. Rather, their status (or, more precisely, their lack of 'legitimate' status) is an unintended consequence of an existing regulatory framework that was never intended to encompass the present reality of non-institutional biology. For better or worse, in opting to peg the screening guidelines to this earlier framework, the Guidance perpetuates this situation.

With a view to these considerations, it is evident that the 'challenges' associated with 'customer screening' go well beyond the technical difficulties encountered in 'sequence screening'. In contrast to sequence screening, customer screening raises questions about a customer's identity, motives, and capabilities – questions that not only draw on unfamiliar areas of expertise among screeners, but also require risk judgments to be made that affect the very subjects they seek to render visible and manageable. In this manner, customer screening, in contrast to sequence screening, is not only technically demanding, but also ethically problematic. Deriving a list of 'denied persons', one might argue, is simply not the same as deriving a list of 'controlled sequences'. Persons, unlike things, exhibit constantly changing 'properties'; they are neither 'sequences' nor 'natural disasters', but rather social actors imbued with human agency – an observation, perhaps, that points as much to the challenges inherent to customer screening as it does to the relative absence of the 'customer' in the screening methodology.

To conclude this section, I wish to return to the subject of human agency, and to the significance of omitting human agency from the risk calculus described in the Guidance. According to the Committee on Methodological Improvements, as discussed earlier, in the absence of knowledge about how 'intelligent adversaries' behave, the DHS opts to model 'persons' as 'things', and, in the process, largely omits

the 'intelligent adversary' from the assessment (NRC 2008). In many ways, this is also true of customer screening. Specifically, in the absence of detailed knowledge about the customer placing the order, screeners draw on a set of indicators, which do not (and cannot) reflect the complexities of the customer in question – an individual who is free to choose his or her own sequence, how they request this sequence, and how they ultimately (mis)use their order if and when it is processed. Thus, while indicators may enable screeners to broadly differentiate between 'legitimate' and 'illegitimate' customers, thus enabling DNA synthesis providers to fulfill their 'due diligence', they also gloss over much of what makes a 'customer' distinct from a 'sequence' – a 'person' distinct from a 'thing'. And, while simplification of complex phenomena is intrinsic to risk assessment in practice (Loasby 1976), and a necessary feature of universalistic rules that strive to maintain business operations and industrial efficiency (Braithwaite 1982), in the case of the *Screening Framework*, I would suggest, the stakes are higher than most.

5.5 Conclusion

The 'screening methodology' developed by the DHHS (2010b) scarcely resembles the strictly 'scientific' approach to science policymaking described in the 'Red Book' (NRC 1983), illustrated as a unidirectional scientific process (see Figure 1). The promise of 'objective' risk assessment, free of 'subjective' human judgment, can hardly be said to reflect the selective processes and administrative logics that enable 'sequences' and 'customers' to be reconfigured as objects of thought and action. To speak of 'sequence screening' in relation to scientific knowledge alone would seem oddly out of place in light of the 'non-biological', 'non-quantifiable' criteria drawn on by the DHHS and the USDA to determine what should count as a 'Select Agent', and, in turn, a 'controlled sequence'. The assorted 'indicators' adopted by screeners to verify a customer's 'identity' with a view to establishing their entitlement to synthetic DNA lacks much of the disinterested 'scientific gaze' so often valued by scientists; promoted as fundamental to the 'scientific process', and favored (if only as a technical ideal) by science policymakers and regulators.

In practice, and in stark contrast to the Red Book's (NRC 1983) idealized representation of risk analysis, the screening methodology described in the Guidance encompasses an array of risk assessment techniques that offer a more or less structured procedure – one that is, above all, 'administrative' or 'managerial' in function – for conducting biosecurity risk assessments, permitting DNA synthesis providers to tick the necessary boxes to ship (or not) orders for synthetic double-stranded DNA. As Power (2007) argues, such 'box-ticking' approaches to risk assessment are 'functional', in the sense that they serve as a more or less formalized process for deriving a risk estimate and making a risk management decision. Moreover, they are 'auditable', in the sense that they serve to explicitly show *how* risk assessments are conducted, providing a formalized proof or justification for taking a particular course of action. In this light, the Guidance, characterized by a 'procedural rationality', can partly be understood as a response to "increased pressures for transparency and accountability", and as an attempt at "blame avoidance" in the event of regulatory failures (Bounds 2010, p. 30).

In this chapter, I have argued that risk assessment in the context of science policymaking is, above all, a pragmatic activity, premised upon the belief that risks can known with reasonable confidence and made the subject of regulatory intervention and control. Although rarely resembling the idealized scientific model of risk analysis – exemplified by 'quantitative risk assessment' – science policymaking is nonetheless concerned with establishing verifiable procedures that can be used to inform and to justify a variety of policy actions, policy actions that cannot be disassociated from the specific risk management objectives they are intended to fulfill, including aspirations for economic development, regulatory consistency and 'blame avoidance'. Moreover, to the extent that these procedures are adopted by industry, supported by federal agencies, codified in policy documents or simply endorsed by various scientific and technical experts who claim to know what should count as the 'best' approach to risk assessment and risk management, they are 'institutionalized' and advanced as new 'standards'. Far from being unique to synthetic biology, this approach to assessing and managing risk, I have argued, has been applied to previous iterations of biotechnology, and, indeed,

is indicative of 'science policy' (Jasanoff 1990) itself, an activity that is, and always was, characterized by a 'mix' of scientific and political considerations.

Yet, as I have also argued in this chapter, the case of synthetic biology is not simply a repetition of what has come before. Indeed, the case of synthetic biology is even distinct from its nearest technological relative, genetic engineering. Today, both the science and the context are perceived to have changed, and scientists and science policymakers envision 'new' risks – risks associated with 'synthetic DNA', 'non-natural templates' and 'deliberate misuse' – while simultaneously imagining 'new' ways of visualizing and managing these risks – by way of adapting (more or less successfully) 'risk technologies' and 'uncertain techniques' (Chapter 2) to contend with the indeterminacies associated with 'sequence information' and the addition of 'human agency' to the risk calculation; by way of establishing lists of 'controlled sequences' and 'denied persons'; and by way of developing administrative procedures based on 'box-ticking' where probabilistic knowledge is unobtainable. While there is no way to neatly summarize these conclusions, what can be said is that risk assessment 'standards' in the context of the life sciences continue to change, embracing an array of risk assessment techniques – both quantitative and qualitative, formal and informal – that are applied and adapted to the management of emerging risks and emerging biotechnologies, even at the 'limits of prediction'. The case of biosecurity risk assessment in the context of the DNA synthesis industry offers one vision of how these diverse techniques are brought to bear on a 'complex problem' in pursuit of 'practical solutions'.

6. Risk management: Preventative controls on science and the limits of the 'classical' biosecurity model

6.1 Introduction

Pragmatism, I have argued, underpins risk management processes directed at the design and development of 'optimal' science policies. In the case of the DNA synthesis industry, this pragmatism is visible in relation to ongoing policy efforts seeking not only to prevent synthetic DNA from being accessed by 'denied persons', but also seeking to achieve this outcome with minimal impact on an emerging industry and with minimal modification to existing regulatory frameworks. Yet, the DNA synthesis industry is only one site where this pragmatic approach to science policymaking is being enacted. Indeed, pragmatism, I suggest, is a common feature of biosecurity considerations, and the regulatory strategies designed to govern synthetic biology. Specifically, questions are being asked by science policymakers, scientists, security experts, bioethicists, and others, about how 'best' to secure and simultaneously sustain an exemplary case of 'dual-use biotechnology', a technology defined by its anticipated capacity for 'bioterrorism' and 'bioeconomy'.

It is, in turn, with a view to this sought-after balance – between 'national security' and 'scientific progress' – that I wish to consider more broadly the risk management options that have been proposed to address the dual-use problem in synthetic biology. In doing so, I wish not only to highlight possible 'options for governance', as they are often referred to in the policy literature (for example, Garfinkel et al. 2007), but, more importantly, to identify their points of agreement and disagreement; their perceived strengths and limitations. Beyond the immediate aim of addressing how diverse groups of experts attempt to negotiate uncertainty and resolve an apparent policy dilemma, this research is intended to examine how risk management strategies are designed and produced in pursuit of particular goals, helping to both orient the 'risk management process' and establish new forms of 'risk responsibility'. In light of this overarching research aim, in this chapter and

the next I will address several questions, including: What risk management options are presently proposed to address the dual-use problem in synthetic biology? What do these options share in common, and how are they different? And, how are various biosecurity interventions justified or contested in relation to potentially competing demands for scientific progress and national security?

With a view to these research questions, I will argue that, while sharing the common objective of enabling a secure and sustainable science, the risk management strategies that have been proposed to date (or, in some instances, that have recently been implemented) seek to achieve this objective in a variety of potentially conflicting ways. Specifically, these interventions range from 'top-down' approaches, premised upon a logic of prevention or precaution and directed at arresting flows of 'dual-use' materials and information (the subject of this chapter), to 'bottom-up' approaches, premised upon a logic of 'prudent vigilance' and directed at shaping scientific conduct (the subject of the following chapter). Significantly, although it cannot be said that 'bottom-up' approaches are necessarily replacing 'top-down' approaches, which continue to be endorsed under the 'classical' biosecurity model, this research suggests that there nonetheless exists a growing belief that addressing the problem of 'deliberate misuse' is likely to benefit less from imposing new restrictions on access to science, viewed by many as threatening norms of scientific openness and potentially limiting scientific progress, and more from encouraging new forms of responsible scientific conduct.

Before proceeding, I should emphasize that the risk management strategies discussed in this chapter and the next are not necessarily viewed as incompatible by their authors. On the contrary, while the various groups of experts engaged in developing biosecurity policies often emphasize one approach to risk management over another, many still endorse aspects of multiple risk management strategies, encouraging what is increasingly referred to as a 'web of prevention' or a 'web of deterrence'.[99] In other words, they tend to endorse an *assemblage* of biosecurity

[99] The term 'web of deterrence' was first introduced by Graham S. Pearson (1993), an international security expert and long-time advocate of chemical and biological weapons disarmament, to describe a range of measures to counter the threat of chemical and

controls, both 'top-down' and 'bottom-up'. As Kwik et al. (2003, p. 32) reason, "governance systems that rely on voluntary standards … cannot, alone, guarantee the prevention of bioterrorism". Conversely, "international treaties or national top-down regulation cannot, on their own, deliver such promises either" (ibid.). Moreover, it should be emphasized that the risk management strategies (each existing at various stages of development and implementation) discussed in this chapter and the next are by no means the only regulatory instruments governing synthetic biology, and modern biology more broadly. Rather, they contribute to "an existing regime, comprised of a collection of cooperative and coercive national and international control measures", including international treaties, national laws, voluntary guidelines and codes of conduct (McLeish and Nightingale 2007, p. 1638). Yet, as many of the biosecurity controls I will discuss remain at an early stage of deliberation, I argue that each intervention (or 'family' of interventions) merits being considered on its own terms. As I will argue, this is because each presents a somewhat different way of understanding and intervening upon biosecurity risks, having different implications for how synthetic biology is governed.

6.2 'Barriers to access': Risk management under the 'classical' biosecurity model

In this section, I will consider a range of risk management strategies for synthetic biology that can broadly be said to fall under the 'classical' biosecurity model. Introduced in Chapter 4, this model is premised upon the belief that (select) biological artifacts (tangible and intangible) are intrinsically dangerous things (McLeish and Nightingale 2007) and that biosecurity controls should (and presumably can) be implemented to prevent them from falling into the 'wrong hands'. These (more or less) 'top-down' approaches to biosecurity are the most common risk management options proposed to address the deliberate misuse of

---

biological weapons proliferation. Presently, the term, which is more commonly referred to as a 'web of prevention', can be found throughout the biosecurity policy literature and was referenced by several experts interviewed for my research.

synthetic biology, and, indeed, to address the dual-use problem in the life sciences more broadly (Reppy 2003). Ranging from the preventative to the precautionary, these include proposals to screen orders submitted to DNA synthesis providers (DHHS 2010b), to review and, if deemed necessary, omit certain research findings in the context of life science publishing (Zilinskas and Tucker 2002), and, indeed, to prevent certain life science research projects from being pursued in the first place if they are deemed to be especially dangerous (Steinbruner et al. 2007).

Although representing a diverse range of biosecurity interventions, which address different aspects of life science research, from controls on biological materials to restrictions on hypothetical experiments, in the following I wish to consider what these options share in common, that is, what binds them together under the classical biosecurity model? At the same time, how do they differ with regard to their specific targets of intervention and control? And, how are they justified or contested in relation to their potential to enable a secure and sustainable science? Drawing primarily on the biosecurity policy literature, and a selection of interviews with science policymakers, scientists and security experts actively engaged in aspects of the synthetic biology policy debate, I will argue that, although these risk management options continue to enjoy considerable support, there exist growing doubts about their capacity to prevent the deliberate misuse of life science research and concerns about their potential impact on scientific progress. In the next chapter, I will then consider an alternative biosecurity model that has begun to gain growing support, a model premised less upon controlling access to science, and more upon influencing scientific conduct, an approach to risk management that is, I suggest, changing what it means to be a 'responsible life scientist'.

In an effort to briefly revisit and further conceptualize the distinctive logics that characterize the contemporary practice of biosecurity, I would like to begin by way of considering the following question: What does a biosecurity intervention that attempts to restrict access to a synthetic gene share in common with a biosecurity intervention that attempts to restrict the publication of research findings describing the *de novo* synthesis of a virus? At a glance, these examples, both of which are familiar biosecurity controls discussed in the context of the

synthetic biology policy debate, would appear to be rather different. After all, the first concerns a tangible entity – a gene – and the second an intangible one – research findings. Although targeting very different 'risk objects' (Hilgartner 1992), what these interventions share in common, I suggest, is a common way of understanding what constitutes a 'biosecurity problem', and, in turn, what constitutes a 'biosecurity solution'. Namely, both interventions view biosecurity in relation to the classical biosecurity model introduced in Chapter 4, which presupposes that there exist various biological artifacts that are, in and of themselves, dangerous things, meriting oversight and control.

For supporters of this approach to biosecurity, barriers to access are perceived to be necessary and (if only tacitly acknowledged by their authors) possible to construct. Constructing barriers to access, in turn, serves as the primary means whereby risks are made the subject of intervention and control. This view of biosecurity, as I argued in Chapter 4, can be conceptualized as a type of 'command and control' activity directed at keeping 'dangerous tools' out of 'dangerous hands'. Conversely, under this model, risks are perceived to arise where there exist gaps or 'vulnerabilities' in biosecurity controls, whether these gaps are perceived to be physical, digital, theoretical or otherwise. As I have argued, this is precisely why synthetic biology is often said to be problematic. That is, it is believed to have the potential to lower barriers to access, whether by 'de-skilling' bioengineering or by enabling the unauthorized acquisition of Select Agents. In turn, perceived differences – 'being a different kind of biologist' (for example, 'non-institutional biologists') or 'doing biology differently' (for example, *de novo* synthesis of Select Agents) – have contributed to an expanding taxonomy of 'risks' that many believe merit being taken seriously and made the subject of risk management.

This view of biosecurity, which essentially describes a mechanism of control or prevention, is clearly visible in relation to the examples I have introduced above; yet, a second observation can also be made with regard to these examples, and this concerns biosecurity's *scope*. Namely, under the classical biosecurity model, genes and research findings, although two very different types of things, are both framed as knowable and governable entities, which can be controlled by way of

constructing barriers to access. In this light, risk management is not so much defined or constrained by the types of 'risk objects' under consideration, but by the specific concepts, categories and ways of ordering used to render these objects amenable to thought and action. Moreover, this approach to risk management, as I argued in the previous chapter in relation to the DNA synthesis industry, is primarily 'administrative' or 'managerial' in function, describing a formalized *process* aimed at producing "a vision of control … and an imperative to manage and be responsible for a newly visible range of problems" (Power 2007, p. 125).

However, while there exist similarities between these two families of biosecurity interventions – the first focused on tangible biotechnologies and the second intangible life science knowledge – there also exist significant differences. Notably, the very fact that information about pathogens (not just physical pathogens) and ideas for experiments (not just experimental outcomes) are now conceived as threats to our collective security is a significant development in itself. Formally existing outside the scope of biosecurity, new concerns about life science knowledge production and dissemination are now the primary sites of a growing number of biosecurity proposals (Atlas and Dando 2006). In other words, the locus of biosecurity has shifted to new domains of the life sciences, domains that are increasingly removed from the tangible entities that are ultimately viewed as problematic, namely, dangerous pathogens. For those engaged in the design and production of biosecurity policies, this shift is coextensive with new anxieties, uncertainties, and dilemmas about an emerging array of 'risks' that must now be brought under a framework of technical intervention and control, while simultaneously ensuring that scientific progress is not diminished. It is, in turn, with a view to how this desired balance might be achieved – both in relation to the more familiar case of tangible biotechnologies and the more recent case of intangible life science knowledge – that I wish to turn to at this time.

6.2.1 Preventative practices: Controlling access to tangible biotechnologies

There exist a range of biosecurity controls (some of which have already begun to be put into practice, while others remain at the inception stage) for synthetic biology that seek to restrict access to tangible biotechnologies (DNA synthesizers, chemical precursors to synthetic DNA, synthetic genes, and so on). Notably, this approach to biosecurity is clearly visible in relation to the Department of Health and Human Services' (DHHS 2010b) *Screening Framework* (discussed in the previous chapter), which prescribes screening procedures and recommends screening software to detect and prevent the unauthorized acquisition of Select Agents (or their constituent parts). In this context, predefined lists of 'denied persons' and 'controlled sequences' serve as practical aids or heuristic devices for risk management decision-making, while much of the responsibility for risk management rests with the 'screener' and their capacities to detect when there exists a mismatch between an ordered sequence and a prospective customer. There also exist, what are rapidly becoming, 'standard' protocols for follow-up and reporting in the event that an order should elicit a 'hit' or a 'red flag', including recently introduced lines of communication with the Federal Bureau of Investigation (FBI). To the extent that the *Screening Framework* is adopted by industry, I have argued, these guidelines provide a standardized risk management procedure defining what should count as legitimate, morally (and, in the case of Select Agents, legally) defensible 'risk-based' government, as well as shifting much of the burden of responsibility for risk management from government agencies and institutions to DNA synthesis companies and their in-house experts.

Although the *Screening Framework* (DHHS 2010b) is currently the most visible, as well as the most detailed, regulatory instrument in relation to synthetic biology, there exist other measures of this kind. Sometimes referred to as 'technical solutions for biosecurity' (Bernauer et al. 2008; Bennett et al. 2009; Kelle 2009), these include not only screening procedures and screening software introduced in the context of the DNA synthesis industry, but also biosecurity proposals aimed at

monitoring and controlling the acquisition and use of specific pieces of equipment and specific chemical reagents that might be used to synthesize synthetic DNA for 'malicious purposes'. For example, in *Synthetic Biology: Options for Governance* (a collaborative policy effort between the US-based J. Craig Venter Institute, the Massachusetts Institute of Technology, and the Center for Strategic and International Studies), Garfinkel et al. (2008, p. 32) propose "methods to monitor and control DNA synthesizers", including registration requirements "(a requirement to notify the government when selling, buying, or otherwise possessing a DNA synthesizer)"; licensing requirements "(government permission is needed before a DNA synthesizer can be acquired or retained)"; as well as registration or licensing requirements "for procuring specialized raw materials (especially the phosphoramidite precursors) necessary for synthesis" and for procuring "key spare parts of synthesizers (such as the capillary tube assembly)". Here, DNA synthesizers (including 'key spare parts') and chemical precursors to synthetic DNA are identified as objects of particular concern, animated with the potential to enable nefarious applications, and made the subject of a risk management proposals that call for more intensive oversight and control of these tangible artifacts.

Similarly, George Church, a Harvard genetics professor and outspoken advocate for biosecurity controls on synthetic biology, proposes licensing DNA synthesizers, as well as monitoring "suspect activities, such as labs requesting DNA that is related to potentially harmful biological agents" and the "purchase of precursor chemicals, nucleic acids, genes and designer cells" (Church 2005, p. 423) that might be used as raw ingredients for producing 'dangerous genetic constructs'. With a view to increasingly technical (if not futurist) modes of surveillance and prevention, Church also proposes using electronic locators to track where DNA synthesizers are located in space, as well as programming DNA synthesizers so that they are unable to produce dangerous sequences (Church, cited in Chyba 2006). Here, Church elaborates a risk management option that might be used to monitor and control flows of 'dual-use hardware', linking this equipment with concerns about 'harmful biological agents' and 'suspect activities'. Other proposals of this kind include building a 'self-destruct mechanism' or 'safety switch' into synthetic

microorganisms, which would be triggered in the event of an unexpected environmental release, disabling "undesirable neo-organisms", with a view to enhancing biosafety and biosecurity (LaVan and Marmon 2010, p. 1010). A further "solution", some scientists argue, "would be to create a [genetic] 'serial number' that could be traced back to individual synthesis laboratories or even individual synthesis machines", verifying a synthetic microorganism's origins (ibid.). According to these scientists, "[s]afety must be designed into the [biosecurity] system", enabling "safe and effective progress within synthetic biology" (ibid.). Bennett et al. (2009) have referred to such approaches as 'safety by design'.

While there exist further proposals of this kind, these represent a characteristic range of risk management strategies that seek to design and produce 'technical solutions for biosecurity'. Although most lack the visibility, level of detail, and institutional support associated with the *Screening Framework* (DHHS 2010b), and therefore may or may not become active regulatory instruments, each attempts to identify specific tangible artifacts of concern and proposes recipes for their management. A relatively common proposal made by scientific and technical experts in the context of the synthetic biology biosecurity debate, these risk management options are nonetheless contested; often with a view to equally positivist arguments put forward by other experts of this kind. Introduced in Chapter 4, the primary critique among scientists, science policymakers, and security experts leveled at these kinds of biosecurity interventions is that they posit that the various tangible artifacts linked with synthetic biology (DNA synthesizers, precursor chemicals, synthetic genes, and alike) can be *both* unambiguously classified (identified, defined, and listed) *and* kept out of the hands of 'terrorists'. Although a desirable possibility, according to many of the scientific and technical experts interviewed for my research as well as the prevailing tide of policy literature on this subject (NRC 2004, 2006, 2011), this view of biosecurity is perceived to be increasingly impractical, if not 'bad', in excess, for science.

These objections, as I touched on in Chapter 4, tend to be justified on the basis of the 'dual-use dilemma', a concept that describes biotechnology's 'latent potential' for both 'good' and 'bad'. It is argued, for example, that biosecurity

controls on tangible biotechnologies are impractical because they require that finite lists of pathogens, genes, laboratory equipment, and so on, be developed, monitored, and periodically updated, while, in practice, biotechnology is said to be inherently 'dual-use', rapidly evolving and globally distributed (Atlas 2005b). Thus, boundaries between 'good' biotechnology and 'bad' biotechnology are not only perceived to be blurred, but also difficult to maintain, monitor and enforce. Moreover, it is agued that biosecurity interventions of this kind, in excess, are disruptive to science (Relman et al. 2006). The argument being, the very biosecurity controls intended to make it difficult for 'illegitimate' actors to gain access to pathogens, genes, chemical precursors to synthetic DNA, and so on, also stand to make it more difficult for 'legitimate' scientists to conduct their work (Atlas and Dando 2006).

Yet, as the previous examples suggest, despite these perceived challenges, preventative controls on tangible biotechnologies are a distinct feature of the synthetic biology regulatory landscape, and, in the case of the DNA synthesis industry, are beginning to be implemented (DHHS 2010b). In this light, the 'dual-use dilemma', contrary to the manner in which the concept is usually framed in life science policy discussions, represents less a source of uncertainty that discourages biosecurity interventions, and more a source of motivation that mobilizes risk management efforts that are adapted to new and emerging risks, new sites of understanding and intervening. While this can be said of biosecurity controls directed at *tangible* biotechnologies, in the following I will argue that in relation to *intangible* life science knowledge there exist an even broader range of risk management strategies, having different implications for how synthetic biology is governed, and generating more pronounced tensions between demands for national security and demands for scientific progress. Significantly, while these strategies remain at an early stage of deliberation (that is, they exist as 'proposals', rather than fully fledged regulatory instruments that have been rolled out by government and adopted by scientists and industry), aspects of these proposals are now visible in the form of new US policy on 'dual-use research of concern' (DHHS 2012).

6.2.2 Precautionary practices: Controlling access to intangible life science knowledge

Discussed in relation to the 'Fink Report' (NRC 2004) in Chapter 4, there exist growing concerns, not only about tangible biotechnologies, but also about intangible life science knowledge falling into the 'wrong hands'. What this means, in practice, I have suggested, is that suspicions about modern biology increasingly relate to the production and dissemination of potentially dangerous information, research findings, scientific protocols, and alike. In turn, the scope of biosecurity has expanded to include new arenas of the life sciences. It was, in fact, with a view to concerns of this kind, and how these concerns might be addressed, that the Fink Committee was convened (under the auspices of the US National Academy of Sciences) to begin with. Specifically, concerns were raised about the publication of several high-profile life science articles that some critics feared would "[alert] bioterrorists to new ways of producing biological weapons and [provide] them with explicit instructions for doing so" (Selgelid 2009, p. 721).

One article, in particular, entitled 'Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template', published in the journal *Science* in 2002, and authored by the virologists Cello, Paul and Wimmer, generated considerable controversy upon publication, drawing attention to the potential risks that might arise if 'terrorists' were to replicate the experiment following the procedures outlined in the scientific protocols. In other words, it was viewed, as several authors have pointed out (for example, Reppy 2003; Atlas 2005a; McLeish and Nightingale 2007; Vogel 2008c), as providing a 'blueprint' or 'recipe' for bioterrorism, as it might enable 'malicious actors' to gain access to a dangerous pathogen. In recent years, this article, and several others linked with synthetic biology,[100] has become synonymous with the concept of 'dual-use research of concern', raising questions about whether some research should be censored prior

[100] Other life science articles that have similarly become inextricably linked with this discussion include: 'Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus' (Tumpy et al. 2005), noted for resurrecting an extinct pandemic virus, and 'Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox' (Jackson et al. 2001), noted for inadvertently engineering a more lethal poxvirus.

to publication, and, indeed, whether some research should be pursued at all (ibid.). In brief, the synthetic poliovirus experiment served as a key vector for debate on the need for biosecurity controls on 'fundamental research'.[101]

Although restrictions on the communication of information related to advances in science and technology are not altogether new, regulatory controls of this kind (which take as their focus the perceived threat of bioterrorism) have, until recently, never been seriously considered in the context of the life sciences (Reppy 2003). To help place the significance of this development in context, in the following I will briefly introduce how potentially dangerous scientific knowledge has historically been made the subject of regulatory control in the US context. I will then briefly underline the key challenges that now face life scientists and life science policymakers who are confronted with a similar set of concerns and dilemmas, which threaten to place national security considerations in conflict with strongly held norms for scientific openness and demands for scientific progress in the life sciences. I will then use the remainder of this section to explore the various policy proposals that have recently been put forward that attempt to enable contentious life science knowledge in synthetic biology (and related research domains) to be managed in such a way that the science can be both secured and sustained.

6.2.2.1 Historical precedents

First, it is widely recognized that the censorship of scientific knowledge is not unprecedented (Atlas 2003, 2009; Rappert 2003; Relyea 2003; Reppy 2003; Gorman 2006; Selgelid 2007). Indeed, in the US context, "information (or secrecy) policy", which focuses on "the need to secure information upon which national security [relies]" (Gorman 2006, p. 62), has historically been deployed to control access to scientific knowledge "bearing directly [or] exclusively on national defense"

[101] In the US science policy context, 'fundamental research' has been defined as: "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community" (National Security Decision Directive 189, 21 September 1985, available at: http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm).

(Relyea 2003, p. 403). Notably, in the case of nuclear technology, restrictions of this kind date back to the Second World War, becoming law under the Atomic Energy Act in 1946 (Gorman 2006). Moreover, a sub-set of this information, perceived to be of greatest relevance to the production of nuclear weapons, has traditionally been "born classified", accessible to only a handful of military scientists and others with security clearance (interview with senior biodefense scientist, David Franz). More broadly, secrecy has become a familiar aspect of the day-to-day workings of security and intelligence agencies, as well as much of the private sector (Roberts 2006). Whether motivated by heightened concerns about national security or demands for industrial growth, information is restricted with the intent of protecting 'intelligence' or 'trade secrets' from falling into the 'wrong hands'.

Nor are policy discussions on the potential conflicts between scientific openness and national security altogether new. In the US context, deliberations of this kind date back to at least the early 1980s. At this time – during the last decade of the Cold War – questions were similarly asked about how to balance demands for scientific openness against demands for national security, albeit with a view to fields of science and technology that were perceived to be especially problematic in relation to possible military conflict with the Soviet Union, including cryptography, very high-speed integrated circuits and artificial intelligence (National Academy of Sciences 1982). Informed by the so-called 'Corson Report' (ibid.), the Regan Administration ultimately decided on a policy approach that, "to the maximum extent possible",[102] would maintain a culture of scientific openness, while reserving the right to classify scientific information of direct relevance to "national security". Enshrined under National Security Decision Directive 189 (NSDD-189), this remains the cornerstone of US policy on scientific communication.

More recently, in the aftermath of 2001 and growing concerns about international terrorism, there has been a renewed emphasis on "secrecy in the interests of national security" (Gorman 2006, p. 58), drawing into focus the underlying dilemma associated with governance measures aimed at censoring

[102] National Security Decision Directive 189. 21 September 1985, available at: http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

science. According to Brian J. Gorman, Associate Professor in the Department of Sociology, Anthropology and Criminal Justice at Towson University:

> "It is widely recognized that science advances at its greatest pace in an open environment where findings are accessible, transparent and replicable by any interested party. The problem, however, is that the open science model is not universally appropriate if it provides terrorists with a free ride from open research in pursuit of malevolent goals." (Gorman 2006, p. 58)

With a view to this dilemma, it is widely argued that, while censorship may mitigate one set of problems, namely the potential misapplication of scientific knowledge by 'terrorists', it simultaneously raises another set of problems. Specifically, familiar concerns have been voiced about governments "over-classifying information to the detriment of much needed transparency" and about undermining the pace of scientific progress due to constraints on the publication process (ibid.).

6.2.2.2 New dilemmas

Second, despite this familiar history, in the context of the life sciences, questions related to the classification of information, much less questions related to the prevention of certain types of life science knowledge from being pursued in the first place due to concerns about bioterrorism, are relatively new (Reppy 2003). Indeed, as the calls for censorship that accompanied the synthetic poliovirus publication made apparent, biosecurity concerns about 'fundamental research' in the life sciences not only mark a discursive shift in the dominant biosecurity frame (traditionally focused on restricting access to tangible artifacts), but also a possible movement towards more 'draconian controls' that could, in "the worst of all possible worlds", both "damage legitimate research and have no significant effect on security" (McLeish and Nightingale 2007, p. 1646). Whether concerns of this kind are warranted, it is apparent that questions are increasingly being posed by life science policymakers, national security experts, and some life scientists (among others) about whether it is appropriate to publish life science research that describes how to construct or manipulate potentially dangerous biological entities.

Moreover, questions are being posed about whether certain research projects should be pursued in the first place in light of their 'dual-use potential'.

With a view to these concerns, life scientists, life science journal editors, and professional bodies representing these groups, have simultaneously been called upon (or, in some instances, have voluntarily taken up the call) to address the perceived risks associated with their work; with the added admonition that if they do not, then federal authorities will, and with a view to implementing biosecurity controls that could undermine long-held norms of scientific openness and limit scientific progress (Atlas 2003; Check 2003; Rappert 2003; Vastag 2003). The challenge now, as one commentator argued during a recent roundtable discussion on "the dangers of keeping genetic information public", is one of determining "what information to oversee, limit, or even prevent and how to do it" (Hunger 2008),[103] while minimizing the "inhibition of critical biomedical advances and the economic development of biotechnology" (Atlas and Dando 2006, p. 282).

6.2.2.3 Managing restraint: What information to prevent, and how to do so?

Although the Fink Report is the most well known proposal directed at preventing the deliberate misuse of life science knowledge – popularizing the concept, 'experiments of concern' – it is by no means the *only* risk management proposal of its kind; nor is it the most restrictive (Atlas and Dando 2006). In recent years, a variety of similar proposals have been made, with synthetic biology cited as a field of research of particular 'dual-use concern' (NRC 2011, p. 21). These include proposals made by security experts in conjunction with life scientists (Zilinskas and Tucker 2002), science journal editors (Journal Editors and Authors Group 2003; Campbell 2006), bioethicists (Douglas and Savulescu 2010), biosecurity advisory bodies (NSABB 2007), and security policy groups (Steinbruner et al. 2007). Whereas some of these proposals have followed the Fink Committee's example, seeking to

[103] Hunger, I. (2008). 'Is the availability of genetic information dangerous?' *Bulletin of the Atomic Scientists*. Roundtables discussion, available at: http://www.thebulletin.org/web-edition/roundtables/is-the-availability-genetic-information-dangerous.

restrict access to information related to a finite number of experiments; calling for life scientists to decide when dual-use risks exist, others seek to anticipate and prevent *any* experiment from being conducted that *might* yield dangerous biological products or information; endorsing independent review panels and external oversight. In each case, while the Fink Report has in many ways set a precedent for others to follow, in no small part because it has helped establish a common vocabulary for the description of 'dual-use research of concern', each proposal represents a somewhat different attempt at defining intangible 'risk objects' and developing ideal frames for their management (Power 2007).

In Table 2, I outline a range of risk management proposals of this kind. Although a non-exhaustive list, these proposals, I suggest, are illustrative of ongoing efforts to develop governance mechanisms that seek to address the 'problem' of 'dual-use research', each of which relates (more or less directly) to synthetic biology. For each proposal, which I have listed chronologically in Table 2, I indicate the source of the proposal (column 1), provide a summary (column 2), identify the specific objects of intervention (or 'risk objects') (column 3), and present the various risk management actions that are advised under the proposal (column 4). In the following, drawing on these proposals as examples, I will consider the manner in which each is designed to offer a rationalized risk management strategy capable of balancing 'risks' against 'benefits'; demands for 'scientific progress' against demands for 'national security'. I will then follow this analysis by way of an example of how a recent controversy related to the censorship of 'dual-use research' has motivated new federal policy that combines elements of these proposals under a single risk management strategy. This development, I suggest, marks a significant step towards the 'institutionalization' and 'standardization' of biosecurity controls that target intangible life science knowledge. Finally, in the last section of this chapter, I will offer a more general critique, advanced largely by social scientists and gaining growing support among biological weapons experts who have begun to increasingly challenge the appropriateness of a 'command and control' approach to biosecurity, concerned less with the content of each proposal and more with their common view of risk management under the classical biosecurity model.

Table 2: Range of risk management proposals directed at controlling the production and dissemination of 'potentially dangerous' life science knowledge.

Source	Risk management proposal	Objects of intervention	Risk management actions
Zilinskas and Tucker (2002) Limiting the Contribution of the Open Scientific Literature to the BW Threat	Restrict dissemination of research results that concern a Select Agent and one of six 'weaponization criteria'; primary responsibility should rest with funding agency and journal editors	Research findings that might be directly relevant to military or 'terrorist' use of pathogens or toxins	Identify 'restricted' research project; restrict dissemination of 'sensitive' portions of published paper; access to restricted material controlled by journal editor in cooperation with funding agency
NRC (2004) Biotechnology research in an age of terrorism ('Fink Report')	Enhance oversight and review of seven 'experiments of concern'; primary responsibility should rest with life scientists	Experiments that might be used to enhance microbial threats	Identify dual-use research of concern; modify research; discontinue research; limit communication of research results
NSABB (2007) Proposed framework for the oversight of dual-use life sciences research	Enhance oversight and review of experiments that might yield one of seven categories of dangerous research products; primary responsibility should rest with life scientists	Experiments that might yield research products that could be directly misapplied to threaten public health or national security	Identify dual-use research of concern; modify research, discontinue research; limit communication of research results
Steinbruner et al. (2007) Controlling dangerous pathogens: A prototype protective oversight system	Implement a tiered system of controls on potential research, matching degree of risk with information disclosure and review requirements; primary responsibility should rest with 'independent' review bodies	Experiments that might yield dangerous pathogens, where a potential pathogen's risk is measured as a function of its anticipated virulence and transmissibility (a measure of its 'intrinsic danger')	Consider extended implications of knowledge to be generated; classify according to three levels of concern; forego research project; limit communication of research results
Douglas and Savulescu (2010) Synthetic biology and the ethics of knowledge	Develop principles for determining when it is ethical to produce and/or disseminate dangerous scientific knowledge ('ethics of knowledge'); primary responsibility should rest with bioethicists	Knowledge generated by synthetic biology that might be deliberately misused, especially knowledge related to the synthesis of 'novel entities', for example, vaccine-resistant smallpox	Do not pursue or disseminate scientific knowledge when risks of misuse are sufficiently high so as to be 'ethically problematic'; select 'appropriate' risk reduction strategies

Before proceeding with my analysis and comparison of the risk management proposals outlined in Table 2, several general observations can be made about these proposals. First, in addition to ascribing to the underlying logics of the 'classical' biosecurity model, the proposals outlined in Table 2 share a further characteristic in common, which I have alluded to already. Namely, they each address aspects of biotechnology that are 'intangible'. In other words, the 'objects' they are intended to control are not biological entities such as pathogens or DNA. They are not even types of laboratory equipment or reagents that might be applied (more or less directly) to the production of such entities. Rather, these objects are more ephemeral types of things, ranging from information transmitted in research protocols to ideas for experiments. Therefore, these biosecurity controls can be thought of as acting upon objects that exist 'upstream' of the tangible biotechnologies discussed in relation to the previous family of controls. In other words, they act upon objects that *could* yield 'downstream' products, such as synthetic genes or genetically modified organisms, if the corresponding information were produced, disseminated and applied to various applications by experienced scientists. At the same time, this relative lack of materiality does not mean, I suggest, that the objects in question are any less 'real' than the tangible biotechnologies discussed previously; much less the biosecurity interventions proposed to control them. On the contrary, the very act of designing and producing new ideas, descriptions, and categories directed at organizing and managing intangible life science knowledge equally constitutes a *practice*. As Hacking (2002, p. 166) observes: as "new modes of description come into being, new possibilities for action come into being in consequence." Therefore, these objects, and the biosecurity interventions proposed to control them, are every bit as significant (and, indeed, 'real') in relation to how synthetic biology can be governed.

Second, while the proposals outlined in Table 2 are directed at similar 'risk objects', these objects are not identical. Rather, the specific objects these proposals are designed to control can be divided into at least three distinct, yet related, categories, which correspond with different 'phases' of life science knowledge

production and dissemination. Listed from the furthest 'downstream' to the furthest 'upstream', these are: types of research findings (Zilinskas and Tucker 2002), types of experiments (NRC 2004; NSABB 2007; Steinbruner et al. 2007), and types of knowledge (Douglas and Savulescu 2010). Although these categories are not as sharply defined as I present them here, and some of the proposals in Table 2 address more than one phase of life science knowledge production and dissemination, these groupings can usefully enable a comparative analysis. A closer look at how each of these objects is conceived as potentially dangerous within the context of each proposal (or set of related proposals), and the risk management actions (column 4) proposed to address these potential dangers, offers deeper insight into how experts produce "visions of 'risk' manageability" (Power 2007, p. 6) through the design of risk management strategies, and how these strategies might affect the communication of life science knowledge in synthetic biology.

Finally, it should also be underlined that the proposals outlined in Table 2 are the product of multiple groups of experts engaged in aspects of biosecurity policy. Characteristic of 'biosecurity policy', which has been described as involving diverse "ecologies of experts and organizations" (Lakoff and Collier 2008, p. 9), the various contributors to these proposals represent multiple institutions, academic disciplines and scientific specialties. With a view to this broad spectrum of policy actors and organizations, it can also be said that biosecurity policy is characteristic of 'regulatory science' more generally. As Irwin et al. (1997, p. 19) suggest, regulatory science is frequently "very heterogeneous in character – in institutional, geographical and specialty terms." At the same time, beyond the institutional and cultural differences that exist between these groups (which contributes to disagreements at the level of what constitutes 'good' or 'better' biosecurity policy) what binds these groups together, I would suggest, is that each views 'dual-use research' as a first-order 'thing' that can be known and made the subject of specific forms of regulation. The following analysis, in turn, attends to these proposals in an attempt to shed light on their points of agreement and disagreement, as well their justifications for what constitutes 'good' or 'better' biosecurity policy.

To begin, the furthest 'downstream' risk management proposals directed at restricting access to life science knowledge concern restrictions on the dissemination of certain types of information that could be transmitted through the publication of research findings. These concerns, as I have suggested, have been linked with several articles that have described synthetic biology experiments, which some fear may provide a 'blueprint' or 'recipe' for bioterrorism, as well as with broader concerns about the open publication of sequence information. Zilinskas and Tucker's (2002)[104] proposal, which relays the findings of a workshop organized by the US-based Center for Nonproliferation Studies and supported by the US Defense Threat Reduction Agency, is illustrative of biosecurity proposals of this kind. "The workshop", according to Zilinskas and Tucker (ibid.), "brought together two groups of professionals who usually do not communicate, the first consisting of scientists, journal editors, and grant administrators and the second of intelligence and security experts". The scope of the workshop, Zilinskas and Tucker (ibid.) note, was to address "possible approaches to minimize the risk that 'sensitive' research findings could be misused for biological warfare (BW) or terrorism."

According to Zilinskas and Tucker (2002, emphasis added), although "[t]he two groups of professionals – scientists and security experts – could not reach a consensus on how sensitive information from scientific research should be handled", most agreed that restrictions on the publication of dual-use research (if any) should be limited to a "small proportion of findings *directly relevant* to the military or terrorist use of pathogens and toxins" – described elsewhere as "'forbidden knowledge'" (Atlas and Dando 2006, p. 282) – in the interest of safeguarding norms of "scientific freedom" and enabling "scientific enterprise" (Zilinskas and Tucker 2002). Based on these considerations, and with a view to NSDD-189 and the existing Select Agent Regulations, workshop participants agreed to a tentative risk management proposal that qualifies "restricted research" as research involving *both* a "Select Agent" *and* one of six "weaponization criteria". Select Agents, as I have discussed previously, include approximately 80

[104] See Zilinskas, R.A. and Tucker, J.B. (2002*). Limiting the Contribution of the Scientific Literature to the BW Threat*, available at: http://cns.miis.edu/stories/021216a.htm.

microorganisms and toxins that have been deemed especially suitable to biological weapons development by the US Department of Health and Human Services and the US Department of Agriculture. The 'weaponization criteria', which are a recurrent feature of the proposals outlined in Table 2 (varying subtly in number and framing), concern modifications to pathogens that could enhance their effectiveness for use as weapons, such as increasing their infectivity, pathogenicity or antibiotic resistance. Based on this conceptual framework, the risk management actions proposed call for life science journal editors, in cooperation with federal funding agencies, to identify manuscripts containing information of this kind with a view to restricting access to "sensitive portions" of the research prior to publication.

What is significant about the design of this proposal, I suggest, is that it effectively subsumes new concerns about dual-use information under the Select Agent Regulations – an existing regulatory framework designed to restrict access to a limited number of physical pathogens – shifting the biosecurity frame from tangible biotechnology towards intangible life science knowledge. At the same time, these concerns are organized around a finite number of 'weaponization criteria' that can be unambiguously defined, listed and reproduced, providing a standard metric for the purposes of risk management. In other words, while one might imagine a far longer list of 'weaponization criteria' (it has been suggested that "microbiology is just one part of research that could be abused", Campbell 2006, p. S20) and choose to align these criteria with any number of dangerous pathogens (not just Select Agents), workshop participants opted for a far narrower definition of what should count as 'dual-use research', endorsing a risk management strategy that is in keeping with institutional and regulatory norms. In this manner, the rationale for this proposal, I suggest, can be traced to its practical capacity to organize and "delineate a conceptual framework for presenting and describing choice and decision" (Power 2007, p. 185). It is, in other words, a further instance of 'pragmatic policymaking' (introduced in the previous chapter); one that attempts to balance demands for security against 'administrative' or 'managerial' conditions that favor standardization and the fulfillment of the risk management process.

Equally significant is the manner in which this proposal (and, indeed, each proposal in Table 2) effectively combines a plurality of (opposing) views on what should count as 'dual-use research' and presents a singular risk management strategy; in this case assigning responsibility for risk management to science journal editors, on the one hand, and federal funding agencies, on the other. Touched on by Zilinskas and Tucker (2002) in their synopsis of the workshop proceedings, referencing the difficulties encountered by the "two groups of professionals who usually do not communicate" in reaching a 'consensus' on the subject of censorship, it is widely argued that scientists and security experts hold very different views, not only on the technical *feasibility*, but also on the *desirability* of censoring 'fundamental research'. While scientists tend to call for greater openness in scientific communication, security experts, it is suggested, tend to call for greater caution (Vastag 2003; Selgelid 2007). Each 'community' – "the security community" and the "academic research community" (Reppy 2003, p. 46) – is also skeptical of the other's contribution to the risk management process, both in relation to their perceived competencies and their professional interests (ibid.).

For their part, scientists argue that security experts and government authorities lack an appreciation for how science is conducted, and thus "scientists cannot rely on the government to define the standards and to establish the right framework for conducting science" (Atlas 2003, p. 16). For example, they argue that research projects, which tend to be represented as 'discoveries' by security experts and public officials, really represent incremental contributions to the advancement of scientific knowledge, and are thus not singularly dangerous (Vastag 2003; Campbell 2006). Moreover, as publication represents only one mode of communication used by scientists (others include informal meetings, academic conferences, and email), they argue that censoring published results alone may be misguided (Campbell 2006). More generally, it is argued that censorship "contravenes a fundamental principle of published science – that it be both open and replicable" (ibid, p. S21). In other words, censorship is perceived to not only go against scientific norms, but also to infringe upon the primary means whereby scientists are permitted to scrutinize colleagues' work and to refute or revise their

research protocols or results (Atlas 2003; Campbell 2006). As Ronald Atlas (2005a, p. 21), former chair of the American Society for Microbiology, succinctly states: "censorship could fundamentally change the very definition of science".

For their part, security experts (among others, for example, ETC Group 2007; Selgelid 2007; Maurer 2011) have questioned the appropriateness of making scientists (including science journal editors) "the guardians of sensitive materials" (Zilinskas and Tucker 2002). They question not only the competency of scientists to engage in aspects of security, a 'field' characterized by its own claims to authoritative knowledge and know-how (Bigo 2006), but also their willingness to limit aspects of life science knowledge production or dissemination. For example, according to one virologist and chemical and biological weapons expert at Harvard University, commenting on possible approaches to restricting the publication of various types of sequence information: "The concept that there might be some information not worth knowing is anathema to scientists" (Kuhn 2008),[105] calling into question the willingness of scientists to make security judgments of this kind. Others have similarly argued that censorship is "antithetical to the scientific spirit" (Enserink and Malakoff 2012, p. 22), which values "both freedom of inquiry and the free sharing of information" (Selgelid 2007, p. 36), and that the concept of "sensitive information" is fundamentally at odds with a life science culture that assumes "an inherent right to know" (Harris and Steinbruner 2005, p. 1). Moreover, as publishing tends to be closely tied to career development, some question to what extent scientists would be willing to place restrictions on their own research (Nexon 2011). In brief, while norms of scientific openness and scientific autonomy are perceived to be essential to science and scientific progress, they are perceived to be problematic in relation to security, thus generating "a sharp dilemma and a fundamental problem of policy" (Harris and Steinbruner 2005, p. 1).

[105] Kuhn, J.H. (2008). 'Is the availability of genetic information dangerous?' *Bulletin of the Atomic Scientists*. Roundtables discussion, available at: http://www.thebulletin.org/web-edition/roundtables/is-the-availability-genetic-information-dangerous.

Taken together, what these points of disagreement or conflict suggest is a more complex picture of 'consensus building' (Stirling 2010) than the formal proposal introduced above might suggest. In this case, as in the case of each proposal in Table 2, there exist points of disagreement between experts about the nature of the risks in question, and about who should ultimately be responsible for guiding the risk management process. Yet, what is perhaps most remarkable, I suggest, is not so much that there exist disagreements between experts (this is hardly uncommon in relation to policy discussions concerning emerging fields of science and technology), but rather that despite these disagreements two very different groups of experts are broadly united in their belief that biosecurity controls of this kind are both necessary and possible. Although in part this might be explained by the very nature of expert advice, which is "usually presented in aggregated and consensual form" (Stirling 2010, p. 1030), it also suggests a willingness on behalf of scientific and technical experts to reach agreement on issues that challenge their individual values in pursuit of a secure and sustainable 'scientific enterprise' (Zilinskas and Tucker's 2002). This shared belief, or at least willingness to compromise, I suggest, is significant in as much as it organizes diverse experts around a common goal, motivating the design and production of risk management proposals (however tentative or loosely agreed they may be) that are presently defining a new constellation of biosecurity interventions directed at controlling the dissemination and production of life science knowledge.

The next furthest 'downstream' set of risk management proposals outlined in Table 2 address the question of whether some kinds of research should be pursued in the first place in light of its 'dual-use potential'. Although the authors of these proposals may equally be concerned about the dissemination of potentially dangerous information, they are, in the first instance, concerned about its *production*. In other words, these proposals are primarily directed at preventing potentially dangerous research from being conducted, or modifying aspects of a research project prior to an experiment, with a view to precluding the need for future censorship of research findings. As Stephen M. Maurer, Associate Professor of Public Policy at Berkeley

University, reasons in relation to this approach to risk management: "Unlike censorship, this strategy can do little to suppress unexpected results. At the same time, it has the practical advantage that a blocked experiment produces no results and is therefore far easier to suppress" (Maurer 2011, p. 1412).

For the authors of these proposals, this approach to risk management is desirable in as much as it requires that scientists, as well as federal funding agencies and other governmental actors and organizations engaged in aspects of biosecurity policy, address biosecurity concerns from the outset of the research process (NRC 2004; NSABB 2007; Steinbruner et al. 2007), avoiding not only the ('primary') risks that might be enabled by the research project itself, but also the 'downstream' challenges, controversies and reputational ('secondary') risks (Power et al. 2009) associated with censoring or classifying 'sensitive' research findings once they have been produced (Enserink and Malakoff 2012). Yet, as one might imagine, and as I will discuss in further detail below, this approach to risk management nonetheless presents its own challenges and dilemmas. Specifically, it can be interpreted as producing a more pronounced tension between scientific freedom, on the one hand, and national security, on the other. In Table 2, I outline three biosecurity proposals of this kind, with the first two proposals (NRC 2004; NSABB 2007) sharing considerably more in common than the third (Steinbruner et al. 2007).

In the case of the first two proposals, the Fink Committee and the NSABB (a biosecurity advisory body to the US government, which was recommended by the Fink Committee in 2004) call for enhanced oversight and review of seven types of experiments – 'experiments of concern' – that might enhance pathogens for use as weapons, all of which (theoretically) apply to synthetic biology. These experiments capture the same 'weaponization criteria' introduced above, but are not strictly limited to experiments involving Select Agents, and therefore apply to a larger field of potential research activities. For some (Steinbruner et al. 2007), the broader scope of both proposals is perceived to be impractical, and possibly disruptive to science, as they not only "capture a wide swath of research", but they also fail to discriminate between the relative risks of individual research projects (ibid, p. 13). For example, two experiments, both employing the same research techniques, might

be categorized as equally dangerous under both proposals, even though one might involve a Select Agent and the other a non-Select Agent. In other words, the Fink Committee's and the NSABB's criteria, which "focus exclusively on research activities, rather than a combination of agents and activities", could result in unwarranted or excessive constraints on research (ibid.). This objection, in essence, appeals to the perceived strengths of the previous risk management option, which presents a narrower definition of 'dual-use research', organizing risk management efforts around a more discrete set of information requirements, thereby providing a stable reference point for the purposes of risk management decision-making.

Irrespective of the specificity of the Fink Committee's criteria (subsequently reproduced and subtly adapted by the NSABB),[106] the very invention of the concept, 'experiments of concern' (as well as, 'dual-use research of concern', an equivalent concept popularized by the Fink Committee), I suggest, is perhaps the most significant aspect of this proposal, as well as the aspect that has been most widely adopted as a category of understanding and descriptor for problematic research in an age of bioterrorism. To describe this concept as an 'invention' is not to suggest that seven types of experiments only recently came into being, or even to suggest that these research activities have only recently come to be viewed as problematic. On the contrary, one can hardly argue that prior to the Fink Report experiments of this kind did not exist; or that there was not a degree of awareness about their potential risks. Rather, in this context, to speak of 'invention' is to suggest that in introducing the concept, 'experiments of concern', the Fink Committee effectively mobilized and focused concerns related to a disparate set of research activities,

[106] The NSABB's seven categories of 'dual-use research' specifically refer to "descriptors of information**,** products, or technologies" (NSABB 2007, p. 18) that might be considered dual-use research if the corresponding pathogen or pathogenic properties were produced, whereas the Fink Committee's categories refer to 'experiments' or 'experimental techniques'. In other words, the NSABB has chosen to modify the Fink Committee's original categories to reflect research *products* as opposed to research *processes*; yet with a view to the same fundamental aim, namely, vetting experiments *before* they are conducted or *before* they are published. Thus, this discrepancy between the two reports, although noted as a significant modification by the NSABB (ibid, pp. 17-18) – "the NSABB categories have a different purpose and meaning from those of the NRC report" – in fact makes little substantive difference.

organizing them around a new set of problems associated with bioterrorism, and linking them with the contemporary practice of biosecurity. In other words, the concept, 'experiments of concern' (as well as 'dual-use research of concern'), has to a large degree enabled these research activities to be understood as 'biosecurity risks', which can and (according to the Fink Committee, the NSABB, and many others) should be assessed and managed. Once again, to draw on Hacking's (2002) conceptual understanding of 'risk' as a performative category or label, risks of this kind – 'experiments of concern' or 'dual-use research of concern' – effectively came into being hand-in-hand with their naming and classification.

Both proposals also agree that life scientists should take primary responsibility for identifying cases of dual-use research, and, in the event that dual-use research is identified, that they should be responsible for implementing 'appropriate' risk management actions. Yet, the NSABB builds upon the Fink Committee's earlier recommendations, specifying a sequence of actions and a set of risk management protocols for scientists and research institutions to follow. In the first instance, they suggest that it should be the responsibility of the principal investigator (PI) to address possible dual-use risks that might arise from their research; in the second instance, the institutional biosafety committee (IBC) where the research is being conducted; and, in the third instance, the NSABB or other "federal government entities" (NSABB 2007, p. ii). Details on how risk assessments should be conducted are also elaborated in the NSABB's report. Provided in Appendix 4, "Points To Consider in Risk Assessment and Management of Research That is Potentially Dual Use of Concern", are a list of supporting questions (essentially a 'checklist') that PIs and IBCs (and, if necessary, the NSABB or other 'federal government entities') may wish to consider in their evaluations of potential research projects, ultimately asking: "Do the potential risks outweigh the potential benefits?" If the answer is, 'yes', the NSABB proposes that they "consider whether the research should be modified or discontinued" (ibid, p. 51).

A distinctly pragmatic question, having significant consequences for the production and dissemination of life science knowledge, the NSABB's own views on the feasibility of this risk management action are ambivalent, or at least they are

ambivalent in relation to the scientific model of risk analysis (discussed in the previous chapter). For example, on page iii, the NSABB asserts that institutional review of dual-use research should involve an assessment of "the likelihood that the information might be misused [and] the potential impacts of misuse", reflecting the scientific model of risk analysis, which calls for a 'quantitative risk assessment' that takes into account the 'probability' and 'consequences' of a potential 'adverse event'. Whereas, on page 2, the NSABB claims that during the course of their own deliberations, "it was not possible to quantify the risk of misuse of information from that research [their own seven 'experiments of concern'], but there was a consensus among NSABB members that there is indeed the potential for misuse". In other words, NSABB members believe there exists a potential dual-use problem associated with seven types of experiments, but one that is impossible to quantify, while at the same time advising that scientists derive a binary answer ('yes/no') to a question that does not lend itself (by their own account) to calculation.

Here, as I have suggested previously, is an approach to risk management that, while continuing to appeal to the vocabulary and methods of 'quantitative risk assessment', has in fact become untethered from this idealized scientific model. In its place, as Power (2007, p. 36) reasons in relation to the "managerial turn" that has come to characterize many domains of contemporary life formally occupied by the "positivism of numbers", is an approach to governing that is more *administrative* – relying on the "organization of uncertainty in the form of frameworks which emphasize management *process*" – than *calculative* (or at least 'calculative' in the narrow sense of 'quantitative risk assessment'). Thus, instead of offering advice on how to conduct quantitative risk assessment (guidance that one might have expected in light of the NSABB's endorsement of quantitative methods) what is proposed is Appendix 4 (NSABB 2007, pp. 51-52) – a 'structured protocol' or 'checklist' that PIs, IBCs, and, indeed, the NSABB itself, are intended to draw upon to determine what should count as 'dual-use research of concern'.

In keeping with the NSABB and the Fink Committee's calls for limited external oversight, and once again with a view to NSDD-189, both proposals also advocate for the "free and open conduct and communication of life sciences

research" and emphasize that "the 'default' position should be the unfettered progress and communication of science" (NSABB 2007, p. 7). However, while both proposals speak to the need for scientific openness and scientific autonomy (an observation that is not altogether surprising in light of the fact that both the Fink Committee and the NSABB have significant representation from life science and research communities, and thus a strong interest in supporting scientific endeavors) the 'risk management actions' under consideration are no less problematic in relation to the communication of life science knowledge. On the contrary, as I have suggested, under both proposals what is at stake is not 'only' the possibility that research findings may be censored once they have been produced, but also the possibility that research projects may be modified or discontinued altogether, effectively arresting flows of life science knowledge production. This represents a distinctly different approach to biosecurity than the previous proposal, which calls for censorship at the point of publication (Zilinskas and Tucker 2002), as biosecurity interventions of this kind are designed to exert their force at the level of the research process itself with a view to validating certain research projects and invalidating others based on possible experimental outcomes (outcomes, as the NSABB suggests, that are foreseeable, but impossible to quantify).

Beyond the fact that predicting the outcome of an experiment prior to conducting the experiment is at odds with the research process in practice, which is characterized as much by chance and serendipity as it is formulaic protocols (a subject I will return to in the final section of this chapter) (Kwik et al. 2003; Suk et al. 2011), some argue that classifying a subset of experiments as 'experiments of concern' could discourage promising research projects from being pursued. For example, according to one prominent synthetic biologist (Rob Carlson) interviewed for my research, an experiment that aims to modify an animal pathogen's 'host-range' for the purposes of developing a vaccine for humans would be qualified as an 'experiment of concern' under both the Fink Committee's and the NSABB's proposals, possibly acting as a "negative incentive" for conducting the experiment. In other words, it is believed that these risk management proposals could have an unintended "chilling effect" on research (ibid.). Other synthetic biologists (Drew

Endy; Andrew Hessel) interviewed for my research raised similar concerns, not only in relation to individual experiments, but also in relation to the field of synthetic biology more generally. These concerns were voiced in terms of the "negative expectations" that might be generated by risk management proposals of this kind, which they believe could "discourage investment" in an emerging bioeconomy or derail promising research initiatives "before they get off the ground".

This approach to biosecurity is taken further in relation to the third proposal of this kind outlined in Table 2. Steinbruner et al. (2007), of the Center for International and Security Studies at Maryland, propose an oversight system that would endeavor to anticipate and prevent *any* research project (not just seven types of experiments) that *might* yield a dangerous pathogen (not just Select Agents). In other words, a finite number of 'experiments of concern' is effectively replaced by an unlimited number of 'experiments that could be of concern'. In this instance, the authors, based on what they refer to as "an intensive effort by a diverse group of scientists, public policy experts, and lawyers to grapple with the many challenges posed by advanced biotechnology" (ibid, Acknowledgments), present different criteria for determining what should count as 'dual-use research'. Specifically, they propose vetting experiments according to "an intrinsic definition of danger" (ibid, p. 23) based on a potential pathogen's (that is, a pathogen that might result from a potential experiment) virulence and transmissibility (two epidemiological properties that they suggest can be used to estimate the risks posed by a potential pathogen, and, by extension, the risks posed by a potential experiment).

Significantly, in relation to the design of this proposal, 'an intrinsic definition of danger' is said to simplify the task of risk assessment.[107] Specifically, it is argued that this approach to risk assessment enables a potential pathogen's risks to be assessed according to just two epidemiological properties (or criteria), offering a

[107] What the authors do not acknowledge is that, given that their proposal effectively applies to an open-ended range of research activities, the task of risk assessment would presumably be significantly more complicated than they suggest. That Steinbruner et al. (2007) do not acknowledge this is ironic given that this 'open-endedness' is precisely what the authors object to in relation to the Fink Committee's and the NSABB's proposals, which they view as too broad (see above).

"basic conceptualization of danger" (ibid.), permitting experiments to be validated or invalidated with relative ease. Yet, this relative simplicity is also said to come at the expense of empirical precision. According to the authors, "any disease outbreak is also affected by environmental circumstances, public health measures, individual immune system reactions and therapeutic treatment", *but*, "for a given set of such conditions pathogens clearly vary in terms of transmissibility and virulence" (ibid.). In other words, the authors point to the more complex social and environmental 'context' that contributes to disease transmission and helps determine the course of a disease outbreak, yet consciously choose to ignore this context in favor of 'an intrinsic definition of danger'. This choice, once again, underlines that risk assessments are not only intended to be reasonably precise (representative of the 'actual' risks), but also practical (achievable with relative ease).

Equally significant, the authors emphasize that the determination of this quotient of danger should reside outside the life science research group conducting the experiment, as "[n]o individual or research team, however competent, honorable, and patriotic, should carry the burden or be given the authority to make research decisions that might put an appreciable fraction of the human species as a whole at risk" (ibid, p. 6). Instead, they call for local, regional and international oversight bodies, composed of "a broadly representative group, including, scientists, security and public health experts and public representatives not directly involved in the research question" (ibid, p. 7). Although limited external oversight is a feature of the previous proposals, in as much as 'federal funding agencies' (Zilinskas and Tucker 2002) and 'federal government entities' (NRC 2004; NSABB 2007) effectively represent 'risk managers of last resort' (Power 2007) who could possibly override scientists' security judgments (for example, they could withdraw funding or recommend censoring published results) in the event of a disagreement or protracted dispute, this proposal envisions a far more limited role for life scientists (at least the ones 'directly involved in the research question') in the risk management decision-making process.

More than a design element introduced to produce a 'better' risk management option, this discrepancy, I suggest, represents a fundamental

difference of opinion about who should be responsible for governing dual-use research. On the one hand, the diminished role of scientists in risk management decision-making is justified on the basis of the risks themselves, which Steinbruner et al. (2007) argue are sufficiently large so as to merit assessment by a group of experts with a broader set of competencies, ranging from national security to public health. Yet, on the other, this diminished role is justified less on the basis of competency (or a lack of competency) and more on the problematic status ascribed to scientists. That is, according to Steinbruner et al. (ibid, p. 3), dual-use information is not only likely to be "extracted from the legitimate research community", but also to be misused by those "trained within that community". Thus, scientists are framed not only as purveyors of 'risky information', but also as 'risky subjects' (a view, as I have suggested previously, that is shared by many contributors to the synthetic biology biosecurity debate, but one that is rarely explicitly stated). In this light, the opinion that, "meaningful protection can only be achieved by imposing some constraint on freedom of action at the level of fundamental research" (ibid, p. 2) represents considerably more than an endorsement of preventative controls on science. Specifically, it reflects an underlying suspicion about what 'freedom of action' might actually mean in the hands – the 'wrong ones' – of some scientists.

Finally, the furthest 'upstream' risk management option outlined in Table 2 describes an effort to identify types of life science knowledge that are perceived to be beyond the scope of legitimate scientific enquiry. According to the University of Oxford bioethicists, Douglas and Savulescu (2010), there exist certain types of knowledge – above all knowledge generated by synthetic biology, which they believe "may be a part of the blueprint for humanity's destruction, easily pieced together by fanatics, psychopaths or ideologues" (ibid, p. 692) – that are sufficiently dangerous so as to be "ethically impermissible". Identifying 'unethical' knowledge, in turn, is said to take priority over 'downstream' risk management efforts that seek to place restrictions on potentially dangerous experiments (NRC 2004; NSABB 2007; Steinbruner et al. 2007) or prevent the dissemination of 'sensitive' research findings (Zilinskas and Tucker 2003). What is needed, Douglas and Savulescu

propose, is an "ethics of knowledge", which takes into consideration not only "empirical facts" about potential risks, but also "questions of value", including values related to "economic growth, scientific freedom and the intrinsic value of knowledge"; considerations, they suggest, that bioethicists are uniquely suited to addressing (Douglas and Savulescu 2010, p. 690).

Although similar to the previous set of risk management options, in as much as this biosecurity intervention (were it to be adopted) would effectively limit the production of scientific knowledge, the authors of this proposal do not attempt to provide a 'scientific' interpretation of 'dual-use research'. Rather, Douglas and Savulescu justify their proposal on the basis of an ethical imperative to not produce knowledge of a particular kind. In other words, they justify their proposal on grounds that exist outside the more familiar (in relation to biosecurity) epistemological domains of biology, public health and national security. In this context, the concept of 'risk' (as conceived under the scientific model of risk analysis) is effectively replaced by that of 'ethics', which is presented as an 'objective' mode of determining an 'optimal' balance between scientific freedom and a range of other value considerations ('value considerations', it must be emphasized, that are no less intrinsic to each proposal outlined in Table 2, and indeed risk analysis processes more generally, even though Douglas and Savulescu suggest that what sets their proposal apart is that it is based on more than 'empirical facts'). Moreover, the authors suggest that bioethicists (neither security experts nor scientists) should play the primary role as arbiters of what types of knowledge are to be considered off limits. In brief, in contrast to the previous proposals, an 'ethics of knowledge' is neither justified on the basis of epidemiology nor on the 'weapons potential of a microbe'; nor does it attempt to derive its authority from the assertions of life scientists or security experts. Rather, it calls on bioethicists "to develop principles [which are not further defined] for determining when producing or disseminating dangerous knowledge is impermissible" (ibid.).

While I have yet to encounter a scientific or technical critique that strictly relates to an 'ethics of knowledge' (a concept, according Douglas and Savulescu, that has yet to receive mainstream attention even among bioethicists), the design of this

risk management option can be further contrasted with the previous proposals in at least three ways. First, an 'ethics of knowledge' (the furthest 'upstream' proposal outlined in Table 2) is a distinctly precautionary approach to biosecurity, as it is directed at controlling the production of life science knowledge at the very point of its conception, before it is tested by way of experimentation, and before it is translated into published results. Therefore, in practice, it would effectively prohibit all 'downstream' research activities associated with that knowledge. By contrast, Zilinskas and Tucker's (2003) proposal, which calls for restrictions on the publication of "findings directly relevant to the military or terrorist use of pathogens and toxins", offers a narrower (and, one might easily argue, more precise) framing of the problem that each proposal ostensibly seeks to address, namely, the deliberate misuse of pathogens. Therefore, in practice, Zilinskas and Tucker's proposal would have a more limited impact on the production and dissemination of life science knowledge. Second, and related to this first point, this proposal is largely disconnected from the potential harms it seeks to prevent, saying little about the epidemiological properties of pathogens and their capacity to inflict harm on public health. Third, an 'ethics of knowledge', which relies exclusively on the reasoning of bioethicists to distinguish between 'ethical' and 'unethical' knowledge, based on unspecified 'principles', shares little in common with the 'process-based' risk management strategies discussed previously, and therefore aligns uneasily with these modes of governing. In raising these points of consideration, I do not mean to suggest that this proposal is any less justifiable than any other, only that biosecurity interventions of this kind would have extensive ramifications for knowledge production and dissemination; are relatively disconnected from the subject matter that is of most immediate relevance to the risks they claim to address, and rely less on 'procedures' and 'processes' and more on 'ethical reasoning'.

In the preceding discussion, I examined a range of risk management proposals (none of which have yet to be directly implemented as regulatory instruments) directed at restricting access to various aspects of intangible life science knowledge. In each case, the authors of these proposals not only attempt to justify the urgency

of 'risks' of a particular kind (for example, 'sensitive research findings') and to propose risk management strategies that might be used to mitigate those risks (for example, 'censoring sensitive portions of manuscripts prior to publication'), but also to justify the 'administrative' or 'managerial' merits of doing so according to their own risk assessment criteria (for example, 'seven experiments of concern') and their own risk management protocols (for example, a 'checklist' enabling the identification and management of 'dual-use research of concern'). In other words, the relative strengths and limitations of each proposal are weighed against each other as much with a view to their practical capacity to enable risk management decision-making, as they are to their technical capacity to objectively 'measure' or 'quantify' risks. In this manner, I suggest, each proposal represents a contribution to an ongoing competition (albeit a 'competition' that is waged as much at the level of an individual proposal's rationalized design as it is at the level of its singular capacity to 'calculate' risks according to the scientific model of risk analysis) to produce a risk management 'standard' that is best suited to the challenges and dilemmas associated with 'regulating' or 'managing' – a distinction that is increasingly blurred (Power 2007) – dual-use research.

Over the last ten years – since the first risk management proposals of this kind began to consider how regulatory authorities might restrict access to 'sensitive' life science research – this competition has contributed to the expansion and diversification of risk management proposals directed at controlling access to intangible life science knowledge. Moreover, each of these proposals promises to achieve an 'optimal' balance between scientific freedom, on the one hand, and national security, on the other. Yet, as I have discussed, these proposals can equally be interpreted as generating a more pronounced tension between these potentially competing objectives, as each of these biosecurity controls seeks to act upon 'risk objects' that exist increasingly 'upstream' of the tangible entities that are ultimately viewed as problematic, namely, dangerous pathogens.

Although it is tempting to suggest that these 'precautionary' strategies reflect a trend towards increasingly restrictive biosecurity policies that will inevitably undermine a culture of scientific openness and diminish scientific progress, as some

fear, this is not necessarily the most likely outcome or even the most accurate representation of the present trend. Rather, what seems apparent in relation to these diverse proposals is a distinctly pragmatic desire to enable a secure and sustainable 'scientific enterprise' (Zilinskas and Tucker 2002); and risk management strategies, whether developed by scientists, security experts, bioethicists or others, have been crafted to make this objective possible. However, which risk management option(s) might prevail as the 'best' mode of governing, and how restrictive "information (or secrecy) policy" (Gorman 2006, p. 62) and a culture of scientific openness might coexist, are nonetheless questions that remain without an answer. And while no single 'answer' is likely forthcoming, recent events have precipitated a US policy response that goes some way towards understanding how an emerging 'standard' for managing 'dual-use research of concern' has begun to take shape, as well as what is at stake in relation to this new standard.

6.3 Institutionalizing 'dual-use research of concern'

On 29 March 2012, the US Department of Health and Human Services (DHHS) released new federal policy on the oversight of 'dual-use research of concern'[108] in an attempt to address a perceived gap in life science regulation, made apparent in light of two controversial research projects that required that 'federal government entities' (notably the NSABB) make security judgments on the question of censoring fundamental research. Reminiscent of the earlier controversy that surrounded the publication of synthetic poliovirus (Cello et al. 2002) (and several other controversial synthetic biology papers published around this time, as I have said), which helped motivate a biosecurity policy debate concerned primarily with the dilemma posed by the publication of 'dual-use research', this most recent controversy has motivated a policy response that attempts to resolve this dilemma. The result, as I will discuss in this section, has been the design and production of a

[108] *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern*, available at: http://oba.od.nih.gov/oba/biosecurity/pdf/united_states_government_policy_for_oversight_of_durc_final_version_032812.pdf.

risk management framework that attempts to balance demands for scientific freedom against demands for national security. Capturing aspects of the proposals discussed in the previous section, this framework, I suggest, can similarly be understood as an attempt to enable risk management decision-making, while remaining within the boundaries of existing regulatory and institutional norms. Yet, before taking a closer look at this new policy, it is important to provide a brief overview of the events surrounding the controversial research projects that helped precipitate this policy response, and which help shed light on the tensions that exist between 'national security' and 'scientific openness'.

6.3.1 Pandemic potential and global controversy

In 2011, two manuscripts under review by the high-profile journals *Nature* and *Science* raised concerns among journal editors about the 'dual-use potential' of the research. Although both journals had in place procedures for addressing potential security issues (motivated by the earlier controversial life science publications, introduced already) (Journal Editors and Authors Group 2003), few manuscripts had previously been flagged for more intensive review (Vastag 2003). Moreover, each of these manuscripts had ultimately been published in full (Campbell 2006; Enserink and Malakoff 2012). However, in this instance, the two studies – one led by Dr. Yoshihiro Kawaoka, of the University of Wisconsin (reviewed by *Nature*), and the other led by Dr. Ron Fouchier, of the Erasmus Medical Center in the Netherlands (reviewed by *Science*), both of which received funding from the US National Institutes of Health (NIH) – were deemed to be especially problematic, raising serious doubts about the appropriateness of publishing the research in full.

The manuscripts in question described the successful synthesis of a more lethal variant – one capable of airborne transmission between mammals – of highly pathogenic avian influenza (H5N1). In recent years, H5N1 has been the subject of intense public health concern and media attention due to its high mortality rate in humans. Prior to these experiments, the virus could only be transmitted through direct contact with infected birds. Although the authors of both studies claimed that

the research was necessary to raise awareness about the pandemic potential of the virus (which was also the NIH's justification for funding the studies in the first place), concerns were simultaneously raised about the open publication of the research and related scientific protocols, as it might enable others to synthesize the virus, providing "a blueprint on how to set off a flu pandemic" (Enserink and Malakoff 2012, p. 20). For many, including many national governments, the World Health Organization (WHO), members of the scientific community, the international media, and members of the general public, the announcement of both experiments highlighted the challenges posed by the communication of dual-use research, and, indeed, whether some types of research should be conducted in the first place (Malakoff and Enserink 2012). Specifically, the question was asked by many: "How do you balance the universal mandate for scientific openness against the fear that terrorists or rogue states might follow the researchers' work – using it as catastrophic cookbooks for global influenza contagion?" (Garrett 2012).

In light of these dual-use concerns, in the fall of 2011, both journals requested the assistance of the US government to help determine what (if anything) should be done to restrict the dissemination of the research. The NSABB was then requested, on behalf of the US government, "to assess the dual-use research implications of [the] two as-yet-unpublished manuscripts"; "to consider the risks and benefits of communicating the research results", and "to provide findings and recommendations regarding the responsible communication of [the] research" (Berns et al. 2012, p. 153).[109] Upon reviewing the manuscripts, a NSABB working group (composed of eight voting members, including scientists and security experts, and a dozen ex-officio members from a variety of federal agencies) (Enserink and Malakoff 2012) concluded that, in both cases, the manuscripts provided sufficient information to enable others, including "those who wish to do harm", to repeat the experiments (Berns et al. 2012, p. 153). This possibility, the NSABB argued, represented a public health and national security risk of "unusually high magnitude"

[109] This editorial (Berns et al. 2012, p. 153), published in both *Nature* and *Science*, was written by members of the NSABB and was intended to, "explain [the NSABB's] recommendations on the communication of experimental work on H5N1 influenza."

and posed a "grave concern for global biosecurity" (ibid.). Yet, the NSABB also argued that the research, which highlighted the pandemic potential of H5N1, "may be valuable for improving the public-health response to a looming natural threat" (ibid.). In light of these considerations, the NSABB unanimously recommended that the basic conclusions of each study should be published, but that the relevant "methods and details", which might permit the experiments to be replicated, should be omitted (ibid.). "The goal", the NSABB argued, "was to deliver the critical information about the H5N1 potential for pandemic spread while minimizing the possible risk that the information could be used for nefarious purposes" (ibid.).

This recommendation was, in the words of the NSABB (Berns et al. 2012, p. 154), "unprecedented", and the decision sparked both "fierce criticism and strong support" (Enserink and Malakoff 2012, p. 20). For supporters of the NSABB's recommendation, censorship was argued to be a necessary (if undesirable) action, as the risk of misuse simply outweighed the benefits of full publication. Critically, for these supporters, omitting the methods sections from the published material was perceived to be an effective means of preventing others from replicating the experiments and thus preventing the deliberate misuse of the research. For critics of the NSABB's recommendation, the decision to censor the two manuscripts was not only argued to set a dangerous precedent, possibly leading to further constraints on science, but also to do little to enhance biosecurity. For many, censorship was argued to be "impossible to enforce and ultimately useless within scientific circles" (Garrett 2012), as scientists could either gain access to the information by other means or already knew the basic techniques needed to conduct the experiments (Enserink and Malakoff 2012). For others, the important question was not so much whether or not restricting access to the information was *feasible*, but rather whether or not it was *desirable*. From this perspective, the call for censorship raised fundamental questions about the role of the state in the "policing of science" (Garrett 2012). For the WHO, the matter of censorship (or, alternatively, full publication) seemed to be a question without a reasonable answer. In a statement

released on 30 December 2011,[110] WHO officials expressed, on the one hand, that they were "deeply concerned" about the possibility that the research might be misused if published in full, and, on the other, that "critical scientific knowledge needed to reduce the risks posed by the H5N1 virus" must increase. Censorship, they feared, might discourage the sharing of information vital to mounting a global public health response to a future H5N1 pandemic. Irrespective of which side of the debate one looked, it was clear that the implications of censorship went "far beyond a couple of paragraphs in a pair of papers" (Enserink and Malakoff 2012, p. 20).

6.3.2 (Re)assessing censorship

"Stung by growing global controversy … and worried about heavy-handed government regulation", H5N1 researchers agreed to a 60 day moratorium on "H5N1 transmissibility research" on 20 January 2012 (Malakoff and Enserink 2012).[111] Likened to the Asilomar Conference, which in 1975 culminated in scientists calling for a temporary moratorium on a range of genetic engineering experiments (discussed in Chapter 5), this call was celebrated by some scientists as an act of prudent self-regulation and dismissed by others as "'strictly symbolic'" and as "'[a]n empty gesture'" intended "'to assure the public'" (biologist Richard Ebright, cited in Malakoff and Enserink 2012). Regardless of the motivation for this self-imposed moratorium – and 'self-regulation' more generally (a subject I will return to in the following chapter) – this act did not address the more immediate problem of what to do with Kawaoka's and Fouchier's controversial manuscripts.

In February 2012,[112] in light of "the global relevance of these issues", the WHO convened a group of experts "to clarify key facts about the studies" and to find "practical, feasible, *ad hoc* solutions to the questions of access to research findings

[110] See 'WHO concerned that new H5N1 influenza research could undermine the 2011 Pandemic Influenza Preparedness Framework', 30 December 2011, available at: http://www.who.int/mediacentre/news/statements/2011/pip_framework_20111229/en/.
[111] This voluntary moratorium was later extended to one year (Malakoff 2013).
[112] See World Health Organization (2012). *Report on technical consultation on H5N1 research issues*, Geneva, 16-17 February 2012, available at: http://www.who.int/influenza/human_animal_interface/mtg_report_h5n1.pdf.

and management of the laboratory-modified viruses." Hearing from members of Kawaoka's and Fouchier's research teams, participating experts were granted "full disclosure" to the uncensored manuscripts and were provided with further details on both studies (ibid.). Satisfied with the value of the work in relation to the advancement of scientific knowledge about the H5N1 virus, as well as the biosafety and biosecurity precautions taken by both research teams, experts agreed that, "from a public health perspective", the unrestricted publication of the manuscripts was preferable to censorship (ibid.). At the same time, participating experts emphasized that the publication of both studies raised "important and valid concerns" about the threat of deliberate misuse, and that ultimately a mechanism that might "realistically resolve concerns about dual-use research" was needed (ibid.). However, "[e]stablishing such a mechanism and implementing it effectively in the very short term was not considered to be feasible" (ibid.). In the interim, it was agreed that Kawaoka's and Fouchier's manuscripts should be published in full, but with two provisions, namely, that greater emphasis be given (1) to the significance and rationale for the studies and (2) to the laboratory precautions undertaken to ensure safety and security during the research process (ibid.).

With a view to the "new and clarified information"[113] generated at the WHO meeting (and, one would be remiss not to add, the global controversy sparked by their initial call for censorship, an observation that does not figure in official statements released by either the NSABB or the NIH), the NSABB opted to reconsider their position on censorship, and extended the same recommendations (the two agreed at the WHO meeting) to both sets of authors. On 29-30 March 2012, the NSABB reviewed the revised manuscripts and unanimously recommended the full publication of the Kawaoka manuscript, and "in a 12-to-6 decision, that the data, methods, and conclusions presented in the revised [Fouchier] manuscript … be communicated after appropriate scientific review and revision" (NSABB 2012, p. 1). In a statement (see footnote 113) released on 20 April 2012, Francis S. Collins,

[113] See 'Statement by NIH Director Francis Collins, M.D., Ph.D. on the NSABB Review of Revised H5N1 Manuscripts', 20 April 2012, available at: http://www.nih.gov/about/director/04202012_NSABB.htm.

Director of the NIH, summarized the NSABB's response to the revised manuscripts and confirmed that both the NIH and the DHHS supported these recommendations. According to Collins, "the information in the two manuscripts should be communicated fully", as "[t]his information has clear value to national and international public health preparedness efforts and must be shared with those who are poised to realize the benefits of this research" (see footnote 113).[114]

While much can be said on the subject of the NSABB's change in position on the question of censorship, what I wish underline here is only that the NSABB's reversal – from calling for censorship to endorsing full publication – did not reflect any changes in the 'risks' themselves. That is, the 'dual-use information' contained in the manuscripts was the same both before and after the authors' revisions. What changed is the manner in which these risks were framed. Specifically, further context was added to the two manuscripts, which made the public health benefits of the research more apparent, and the biosafety and biosecurity precautions taken more explicit, offering a more favorable interpretation of the 'risk/benefit calculations' used by the NSABB to justify their decision. For critics of the NSABB's initial call for censorship, this (re)assessment or (re)interpretation of the two manuscripts (and, in turn, the 'risks' they are claimed to have contained) merely underlined what was evident from the very beginning, namely, that the NSABB's recommendations were made on the basis of 'expert opinion', and not on the basis of an 'objective assessment' of the 'actual' risks (or, for that matter, the 'actual' benefits) of publishing (or not publishing) the research. As one science blogger, biologist Vincent Racaniello,[115] expressed after the NSABB's initial call for censorship, reflecting a sense of frustration about the lack of transparency related to the risk assessment 'methods' used by the NSABB to arrive at their conclusions: "What data did they consider when making this decision? What were the benefits

[114] The Kawaoka article (Imai et al. 2012) was ultimately published in *Nature* on 21 June 2012 and the Fouchier article (Herfst et al. 2012) in *Science* on 22 June 2012.
[115] See 'The NSABB speaks on influenza H5N1. Virology Blog: About Viruses and Viral Disease', 31 January 2012, available at: http://www.virology.ws/2012/01/31/the-nsabb-speaks-on-influenza-h5n1/.

and the potential harms, and how did they weigh them? Apparently we must take the word of the panel that they reached the right decision."

Based on the NSABB's own account of their initial call for censorship, it is, indeed, difficult to discern any formal 'methods' for conducting the 'cost/benefit calculations' they claim to have used to arrive at their conclusions (Berns et al. 2012). The NSABB says only that the working group assessed "the risks and benefits of communicating the research results", and because of the "significant potential for harm in fully publishing [the] results", and because this harm "exceeded the benefits of publication", "we therefore recommended the work not be fully communicated in an open forum" (ibid, p. 154). Reference to risks of an "unusually high magnitude" (ibid.), although suggestive of the vocabulary common to 'quantitative risk assessment', does not in itself say anything about how the risks were 'calculated', or even whether 'quantitative' methods were used.

In their account of their reversal of their initial call for censorship, however, the NSABB (2012) is more forthcoming about their risk assessment methods. Specifically, the NSABB refers to "analytical frameworks" used to arrive at their decision to publish both manuscripts in full (ibid, p. 2). Under closer inspection, these 'analytical frameworks' (noted in footnotes 3 and 4 of the NSABB's recommendations) reveal themselves to be none other than the NSABB's own *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information* (NSABB 2007, outlined in Table 2 and discussed in the previous section). Presumably, the 'analytical frameworks' they are referring to are contained in Appendix 4 (ibid, pp. 51-52): "Points To Consider in Risk Assessment and Management of Research That is Potentially Dual Use of Concern". As I discussed earlier, Appendix 4 is a 'checklist' or 'structured protocol' intended to help PIs and IBCs (and, if necessary, the NSABB or other 'federal government entities') determine what should count as 'dual-use research of concern', enabling an 'either/or' risk management decision – either to 'modify' or to 'discontinue' the research. It does not, however, represent an 'objective' means of determining the 'actual' risks or (for that matter) the 'actual' benefits enabled by an experiment, even though 'quantitative' methods are

variously endorsed and contested (on the basis of the NSABB's own experiences trying to employ these methods) throughout the oversight framework (ibid.).

To summarize the NSABB's (2012) account of the decision-making process that led to their decision to recommend full publication after their initial call for censorship: the NSABB working group assessed both revised manuscripts according to the NSABB's own oversight 'checklist' (NSABB 2007), which revealed that what was once 'dual-use research of concern' was no longer 'dual-use research of concern', and not because of any changes in the 'risks' themselves, but because further context, which emphasized the 'benefits' of the research and the biosafety and biosecurity precautions taken during the research process, was added, which, in turn, shifted the balance of the 'cost/benefit calculations' (NSABB 2012).

For the NSABB, the NIH, and the WHO, what this recent experience has underlined is an apparent gap in life science regulation, rendered visible in light of the lack of a risk management standard that could effectively address the challenges, dilemmas, and global controversies associated with governing dual-use research. According to the NSABB (2012, p. 6), following their reversal on the question of censorship: "The need for an effective, practical, and feasible mechanism for selectively sharing sensitive scientific information has never been more apparent".[116] In turn, it is precisely this perceived deficiency that has motivated the US government to move quickly to establish (or attempt to establish) a rationalized, morally defensible, risk management strategy that might be used to prevent future 'primary' and 'secondary' risks associated with the publication of controversial dual-use research. From the perspective of regulators, the recent controversy has made apparent that a federally mandated standard (or, in the case of the WHO, an internationally agreed standard) for screening dual-use research – *well before the point of publication* – is urgently needed to avert not only potential public health

[116] This need is made all the more apparent in light of the NSABB's belief that, while full publication was justified in this instance, "research findings will likely emerge in the very near future that should not be widely disseminated because of a high risk of misuse but that nevertheless should be made available to certain researchers and public health officials around the world who have a legitimate need to know" (NSABB 2012, p. 6).

risks, but also the reputational risks associated with the problematic task of censoring 'sensitive' research findings once they have been produced. Made equally clear during this experience, is that any such standard will need to carefully balance potential tradeoffs between national security and scientific freedom – a goal that would seem, at least for the time being, to be anything but straightforward.

6.3.3 The policy response

The *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern* (DHHS 2012) represents an attempt to produce just such a standard. Announced at the close of the NSABB's deliberations on Kawaoka's and Fouchier's revised manuscripts, "[t]he fundamental aim of this oversight is to preserve the benefits of life science research while minimizing the risk of misuse of the knowledge, information, products or technologies provided by such research" (ibid, p. 1). Although the policy overview only acknowledges the NSABB's (2007) earlier proposed oversight framework as helping guide the design of this new policy, reflecting the institutional links that have been established between the US government and its primary biosecurity advisory body, this risk management framework captures aspects of each proposal outlined in Table 2. Also like these proposals, this framework can be understood as much as a pragmatic attempt to enable choice and decision (Power 2007), as it can an attempt to 'objectively' assess and manage the 'actual' risks posed by 'dual-use research of concern'.

Like previous proposals of this kind, the new federal policy endeavors to make new concerns about intangible life science knowledge 'fit' existing institutional and regulatory norms. As described in the policy overview (DHHS 2012, p. 1), the new risk management framework is intended to compliment "existing United States Government regulations and policies" (notably, the Select Agent Regulations and existing federal funding arrangements) and seeks to produce "flexible approaches that leverage existing processes, and endeavors to preserve and foster the benefits of research." To achieve this objective, the new framework is organized around the existing oversight model established for federally funded life

science research. Specifically, federal departments and agencies that fund life science research, which already conform to "regulations and policies governing the possession and handling of pathogens and toxins [in other words, Select Agents]" (ibid.), must now also be aware of, attempt to identify, and implement "risk mitigation measures" to address, 'dual-use research of concern' in current and future research projects (ibid.). As outlined in the new policy, these new 'risk mitigation measures' can include anything from enhancing biosecurity efforts during any stage of the research process (decisions that will be made in collaboration with the participating scientists and scientific institutions) to requesting the censorship of published results, classifying research in accordance with NSDD-189, or terminating (or simply not providing) research funding (decisions that will be made by federal departments and agencies alone).

Also like previous proposals of this kind, the new risk management framework sets out a finite list of criteria that are intended to enable risk management decision-making. Specifically, the framework defines 'dual-use research of concern' as research involving one or more agents or toxins (15 in total) *and* one or more categories of experiments (seven in total). These two sets of criteria, both of which can be found in earlier proposals, provide a standard metric for the purposes of risk management, while simultaneously linking existing concerns about a finite number of pathogens and toxins with new concerns about particular types of experiments or experimental techniques.

In relation to the list of agents and toxins, which serve as the first set of criteria, it is noteworthy that only 15 pathogens and toxins are included under the new framework, instead of the approximately 80 currently listed under the Select Agent Regulations. In contrast, a number of previous proposals defined dual-use research in relation to the complete list of Select Agents (for example, Zilinskas and Tucker 2002), or chose to abandon the Select Agent list altogether (for example, Steinbruner et al. 2007). Under the new framework, the shorter list of agents and toxins produces a definition of 'dual-use research of concern' that is relatively narrow, limiting the scope of the policy, while simultaneously enabling risk management decisions to be made based on fewer information requirements. As I

have discussed in relation to previous proposals, a narrower definition of dual-use research, while perceived to be practical, is also criticized for being less comprehensive. Equally noteworthy are the specific pathogens and toxins that makeup this list. In addition to a number of 'classical' biological weapons candidates (anthrax, smallpox, Ebola virus, and so on), the list also includes "Avian influenza (highly pathogenic)" and "Reconstructed 1918 influenza", which are more recent additions to the biological weapons discussion. The inclusion of these 'newer' biological weapons candidates, especially in light of the framework's shorter list of agents and toxins 'of concern', not only reflects an active interest on the part of the US government to address the earlier controversies surrounding these biological entities, but also renewed concerns about the synthetic biology techniques that enabled their synthesis. In effect, these pathogens, and the synthetic biology techniques used to construct them, have been identified – indeed, they have been *institutionalized* – as 'risk objects' of particular 'dual-use concern'.

In relation to the seven categories of experiments, which serve as the second set of criteria, this list has essentially been conserved from previous proposals. Although the language adopted in the new policy to describe these seven problematic research endeavors most closely resembles the language used in the NSABB's (2007) earlier oversight framework, these categories reflect the same 'weaponization criteria' presented in the earliest proposals directed at controlling access to various aspects of life science knowledge (for example, Zilinskas and Tucker 2002). Yet, while these categories have been highly conserved between proposals over the last ten years, reflecting broad (or at least tacit) agreement on the types of research activities that are most problematic, their use in the new federal policy further validates and reinforces their perceived legitimacy, and, indeed, moves them one step closer to becoming a regulatory 'norm' or 'standard'. Consequently, today, more than ever before, a formally disparate set of experiments and experimental techniques, increasingly known as 'experiments of concern' or 'dual-use research of concern', can be said to have emerged as a distinct category of understanding and intervening – one that describes and simultaneously produces

'risk objects' of a particular kind, which can, in turn, be defined, listed, reproduced, and used as a standard metric for the purposes of risk management.

In relation to the specific protocols or procedures for conducting risk assessments and making risk management decisions on 'dual-use research of concern', the new oversight framework largely defers to the earlier oversight framework produced by the NSABB (2007). "For additional guidance on how to conduct the risk assessment", the new federal policy states, "departments and agencies may refer to the 'Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information', which identifies useful assessment tools" (DHHS 2012, p. 4). As I have already discussed the NSABB's (2007) oversight framework (especially Appendix 4, which provides a 'checklist' for assessing and managing 'dual-use research of concern'), I will not comment at length on the new federal policy's endorsement of this method of deriving biosecurity risk estimates, and making biosecurity risk judgments. I will only say that, in endorsing this particular approach to risk management – one that is as much 'administrative' or 'managerial' as it is 'calculative' (in the sense implied by 'quantitative risk assessment') – the new federal policy has, for better or worse, privileged one way of thinking about and acting upon 'dual-use risks' at the expense of others. As the authors of an editorial published in *Nature* in 2006 expressed about the NSABB's checklist, while "hardly profound or original", "what's new is the idea that such a checklist should itself be widely disseminated to raise awareness and to help peer reviewers, university administrators, students, government officials and experienced investigators examine research critically" (Nature 2006, p. 715). Under the new federal policy, this observation would appear to be further reinforced.

In light of this brief (comparative) analysis of the recent federal policy, it seems apparent that the *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern* (DHHS 2012) is not the first risk management framework of its kind. It is not altogether 'novel' or 'inventive'. Previous proposals (see Table 2) have attempted to develop risk management strategies that seek to restrict access to various aspects of life science knowledge deemed to pose

biosecurity risks. A number of these proposals, in fact, would appear to have done much of the conceptual work of defining various 'risk objects', grouping them together into categories, and developing rationalized strategies for their management. Yet, its lack of novelty does not make the recent federal policy unimportant. On the contrary, in relation to federally funded research in the US (and one can only speculate as to how far this new policy may be extended to non-federally funded research projects in the US or how far it may travel internationally), the new policy defines a new space for regulatory intervention. Moreover, as Bounds (2010, p. 22) suggests: "Once regulatory or policy solutions have been identified and become owned by stakeholders it is extremely difficult for alternative approaches to be given serious consideration even if their merits are supported by robust analysis." Thus, to the 'Select Agent Regulations', I would suggest, one might also add the new federal policy on the oversight of 'dual-use research of concern', and with it, new concerns and dilemmas related to the production and dissemination of intangible life science knowledge. The new federal policy has, in essence, institutionalized the concept 'dual-use research of concern', and validated a set of risk management practices directed at controlling access to life science knowledge, from the conception of an idea for an experiment to the publication of research findings. In the balance, are controversial choices related to national security and scientific freedom; and, as recent experience suggests, potential tradeoffs between these two objectives pose a clear dilemma.

6.4 Beyond the 'classical' biosecurity model: Reframing 'biosecurity'

As I have suggested, there exists a more general critique that applies to both families of risk management strategies that I have discussed in this chapter (and throughout much of my thesis). This critique, advanced largely by social scientists and gaining growing support among biological weapons experts (for example, Tucker 2011) and other scientific and technical experts contributing to biosecurity policy discussions in the US context and beyond, relates to the common way in which biosecurity proposals under the classical biosecurity model conceptualize the problem posed by

biotechnology. Specifically, as the science and technology scholars McLeish and Nightingale (2007, p. 1644) observe, "the traditional way of thinking about dual use policy" is in terms of "technology transfer". This way of thinking reflects the belief that technology has "intrinsic (fixed) functions" that can be applied in benevolent or malevolent ways with relative ease (ibid.). Consequently, the policy problem is "understood in terms of ... preventing *intrinsically* dangerous research and technology getting into hostile hands" (ibid, emphasis in original). Of particular concern in relation to the classical biosecurity model, as I have shown, are questions of access to the material or informational elements that makeup modern biology, ranging from pathogens and oligonucleotides to reagents and DNA synthesizers, as well as codified knowledge, such as information found in journal articles, scientific textbooks, genomic databases, and alike (Vogel 2008a).

This way of understanding biosecurity reflects the prevailing logic of the 'dual-use dilemma', a concept that infers that biotechnology embodies a 'latent potential' for 'good' and 'bad'. It is also the way in which the security risks posed by other advanced technologies (for example, nuclear technology and its application in the production of nuclear weapons) have traditionally been conceived, as well as the arms control regimes that have been invented to manage these risks (McLeish and Nightingale 2007). Yet, this approach to security, one that is premised upon restricting access to intrinsically dangerous artifacts, at least in relation to the life sciences, is increasingly contested. Not only is this because biotechnology is perceived to be widely accessible (motivating some to argue that biotechnology cannot be kept out of the hands of 'terrorists'), but also because it is perceived to misrepresent how science is conducted in practice. In practice, life science research, especially advanced research in synthetic biology and related fields of biotechnology, requires considerably more than access to equipment, reagents and scientific protocols. In particular, it is said to require tacit knowledge, teamwork, and even a degree of luck (Vogel 2008c), which are all 'ingredients' in relatively short supply. Acknowledging that this is the case, in turn, complicates the dominant biosecurity frame, and opens up space for alternative biosecurity models.

The work of the sociologist Kathleen Vogel has helped shed light on some of the underlying challenges that make advanced biotechnology difficult to exploit for malevolent purposes (or, for that matter, for benevolent ones). For example, some of her fieldwork has looked at the contingencies that were encountered by the Wimmer research team in producing synthetic poliovirus (Cello et al. 2002), which, as I have said, generated considerable controversy upon the publication of the results and accompanying scientific protocols. "When the poliovirus experiment is discussed in policy circles," Vogel (2008c, p. 48) observes, "the focus tends to be on how the Wimmer group obtained information about the genome sequence off the Internet and ordered commercially available oligonucleotides to make the virus". Yet, based on her interviews with members of Wimmer's research team, the research experience was anything but straightforward.

According to Vogel (2008c), certain aspects of the synthetic poliovirus experiment, especially difficulties encountered in isolating the cell-free extracts needed for several viral assembly steps, were perceived to be especially challenging, requiring that the virologists develop "particular intellectual insights, laboratory practices, team-work, and trouble-shooting efforts" (ibid, p. 49) to overcome these obstacles. Therefore, the success of the experiment, Vogel argues, was not so much "based on cutting edge technologies", but on "evolutionary and well-established laboratory practices and techniques" (ibid.). Of particular importance, she suggests, was the role of 'tacit knowledge', which, unlike 'explicit knowledge', cannot be communicated in writing, but must be learned through practice and trial and error. Therefore, even though published in full, including step-by-step instructions on how to produce 'cell-free extracts', Vogel's research suggests that the Wimmer article is not (as it is sometimes claimed) a 'cookbook for bioterrorism' (ibid.).[117] Although equivalent fieldwork has yet to be undertaken on the controversial H5N1 experiments, which drew similar concerns about providing 'recipes for

[117] According to Wimmer (cited in Vastag 2003), what is also often overlooked is that his research team's synthetic poliovirus was considerably less virulent than the naturally occurring variety, reflecting not so much the unqualified success of the experiment (and, in turn, the efficacy of synthetic genomics), but rather its challenges and limitations.

bioterrorists',[118] a closer look at the social and technical challenges encountered during these experiments might equally temper concerns about the deliberate misuse of the published findings and scientific protocols.

This more nuanced picture of what it takes to (mis)use synthetic biology in practice – that is, a perspective that takes into consideration the social context and indeterminacies associated with advanced bioengineering work – has been adopted by some biological weapons experts and advanced in their own arguments that question the basic assumptions underpinning the classical biosecurity model. In his article, 'Could Terrorists Exploit Synthetic Biology?', Jonathan B. Tucker, a former chemical and biological weapons expert, credits Vogel's work, emphasizing that the need for tacit knowledge may effectively go against synthetic biology's 'deskilling' agenda, limiting its potential for deliberate misuse (Tucker 2011). Although some commentators – often drawing on synthetic biologists' voiced expectations for revolutionary advances in biotechnology and predictions of "easy-to-use tabletop synthesizers" (Maurer 2011, p. 1400) – express the belief that synthetic biology will inevitably 'black-box' the various steps required to synthesize a virus, thereby diminishing the need for tacit knowledge and enabling bioterrorism (for example, Chyba and Greninger 2004; Chyba 2006; Gorman 2006), according to Tucker this view of synthetic biology is, if nothing else, premature:

> "To date, the de-skilling of synthetic genomics has affected only a few elements of what is actually a complex, multi-step process. Practitioners of *de novo* viral synthesis note that the most challenging steps do not involve the synthesis of DNA fragments, which can be ordered from commercial suppliers, but the assembly of these fragments into a functional genome and the expression of the viral proteins." (Tucker 2011, p. 72)

Similarly, the NSABB, in contrast to many of their statements on synthetic biology, which appear to lend support to the underlying assumptions of the classical biosecurity model, has suggested that:

---

[118] For example, Robert Webster, a flu scientist and advisor to the NSABB during their deliberations on the H5N1 manuscripts, expressed that: "'I don't think science should be putting out recipes' for bioterrorists" (cited in Eserink and Malakoff 2012, p. 22).

> "[Although the] technology for synthesizing DNA is readily accessible, straightforward and a fundamental tool used in current biological research … the science of constructing and expressing viruses in the laboratory is more complex and somewhat of an art. It is the laboratory procedures downstream from the actual synthesis of DNA that are the limiting steps in recovering viruses from genetic material." (NSABB 2006, p. 4)

In practice, Tucker (2011, p. 73) has argued, "only a limited number of scientists have the requisite skills and tacit knowledge" needed to effectively achieve a successful experimental outcome using this technology.

Several synthetic biologists interviewed for my research also share this view. According to Rob Carlson, who has gained considerable recognition for modeling both the rapidly falling costs of DNA synthesis and its increasing productivity (Carlson 2009), a projection that has motivated equal measures of hope and anxiety about the potential (mis)applications of synthetic biology:

> "If you go talk to people who build viruses for a living – who build those flu viruses; who are funded to the tune of tens of millions a year, and have dozens of people working in their labs – they fail a lot. They fail most of the time. The vast majority of the time their experiments don't work. The notion that, say, in the zero to five year time period, 'anyone' will be building artificial pathogens, or even rebuilding naturally occurring pathogens, is not credible." (Rob Carlson)

From the perspective of DIY-biologists (also known as 'biohackers', a name embraced by some members of this community, but one that often carries pejorative connotations in the context of biosecurity), who do not have access to comparable financial or technical resources, this assessment is said to be especially true:

> "[DIY-biology] has turned out to be far more difficult than many people expected, to actually get anything up and running, even basic stuff, like DNA extraction and things like that. I mean biology is hard. It's really hard to do successfully, particularly when you're trying to do it on a budget of 100 dollars and with household materials … and if you were to read the protocols of any published paper and then go in your own lab and try to reproduce those …

> they leave so much out, there's so much left to be desired, because there's a lot of it that's tacit knowledge that took months and months of work, and that they may gloss over in the description of their methods…" (Jason Bobe, co-founder of DIYbio)

In this light, DIY-biologists, who are perhaps the most scrutinized individuals in relation to the possible deliberate misuse of synthetic biology, take on a different image – from nefarious 'biohackers' working with synthetic pathogens in the garage to 'hobbyists' struggling to make even simple experiments work.

There then exists a further dimension that is often glossed over by biosecurity proposals that ultimately seek to restrict access to pathogens; namely, 'access to pathogens' is not synonymous with 'access to biological weapons'. According to Tucker (2011) (see also Tucker and Zilinskas 2006), successfully synthesizing a virus is only the first step towards producing a biological weapon. The remaining steps, including culturing sufficient quantities of the desired biological agent, "formulating the agent with chemical additives to enhance its stability and shelf life", "processing the agent into a concentrated slurry or dry powder", and developing a suitable delivery system "that can disseminate the agent as a fine-particle aerosol that infects through the lungs" (Tucker 2011, p. 73), are perceived to be equally challenging, and equally dependent upon tacit knowledge. In fact, according to a number of biological weapons experts (David Franz and three other senior biodefense scientists interviewed for my research), these steps are far more of an 'art' – "known by few, and practiced by even fewer" (David Franz) – than the task of constructing infectious microorganisms, which, as I have said, many consider an 'art' itself. "If you take your thinking all the way through the con-ops (the concepts of operation)," David Franz explained about the challenges of producing viable biological weapons, "the risks look very different".

Moreover, and in stark contrast to the dominant biosecurity frame, a number of biological weapons experts interviewed for my research believe that some aspects of biological weapons production are far more dependent upon "the old profession of weapons development" (David Franz) than they are cutting-edge biotechnology. For example, in a revealing discussion (held during a recess of the

BWC) with one senior biodefense scientist and biological weapons expert, he explained that he sees little value in restricting access to synthetic biology; not only because the science is perceived to be relatively complicated, but also because it is perceived to be less 'useful' than some of the tried and tested techniques (referred to as, "the dark arts") developed in the context of former biological weapons programs. By contrast, he (and David Franz expressed a similar view) does advocate for the classification of "practical information" that relates to some of the "old tools" used by these programs (for example, techniques used in the "environmental stabilization of organisms"), which he believes have "no real value for the legitimate life science community", and may actually pose a significant risk.

This view is similarly expressed in a recent study by a group of biological weapons experts who endeavor to look beyond the question of 'access' to advanced biotechnology to address the question of how this technology might actually be exploited (or not) in practice. In this study, the authors (Suk et al. 2011, p. 1) "reviewed 27 assessments (published between 1997 and 2008) that address the links between life science research and bioterrorism" with a view to ranking these assessments according to the level of expertise and technical infrastructure that would likely be needed to successfully perpetrate each attack. According to the authors, while the vast majority of the published assessments focus on the deliberate misuse of advanced biotechnology, they fail to adequately consider the level of expertise and technical infrastructure that would (based on their own assessments) be needed to successfully misuse the technology. Contrary to the dominant biosecurity frame, which privileges 'high-tech' acts of bioterrorism, their research "suggests that 'low tech' activities may be especially attractive to bioterrorists", as these could most easily be exploited (ibid, p. 2). Moreover, as one of the authors of this report (Iris Hunger) expressed during an interview:

> "The historical record also suggests that terrorists will use simple methods. So, first of all, they will take what's there ['for example, pathogens found in nature'], and not create something new ['constructing a novel pathogen using synthetic biology or genetic engineering techniques'], and then distribute it in a way that's fool proof ['for example, contaminating food']." (Iris Hunger)

Emphasizing the importance of tacit knowledge, and its limited availability, Suk et al. (2011, p. 3) conclude that, "[b]iosecurity policy discussions could gain more nuance and credibility by adopting more sophisticated notions about the challenges inherent in conducting and replicating advanced research."

Taken together, these views suggest that the deliberate misuse of synthetic biology (and biotechnology more broadly) is more than just a question of 'technology transfer'. In other words, *access* to biotechnology (tangible or intangible) does not necessarily, in and of itself, constitute a 'biosecurity problem'. Conversely, *restricting access* to this technology, which is the fundamental tenant of the classical biosecurity model, does not necessarily, in and of itself, constitute a 'biosecurity solution'. Significantly, this alternative framing of the problem posed by biotechnology not only represents a form of technical critique, calling into question the *feasibility* of biosecurity interventions based on the classical biosecurity model, but also suggests the possibility of other modes of intervening upon biotechnology that may be more *desirable* in relation to balancing potentially competing demands for national security and scientific progress. After all, for some, as a number of the arguments discussed in this chapter suggest, biosecurity controls aimed at restricting access to science, especially intangible life science knowledge, are not only technically demanding to implement, but also potentially counterproductive, as they may limit scientific openness and diminish scientific progress.

In this light, there exists growing interest in alternative approaches to biosecurity, ones that move beyond the classical biosecurity model. In particular, there exists a growing belief that what is needed are biosecurity interventions that rely less on 'top-down' risk management efforts that seek to restrict access to science, and more on 'bottom-up' risk management efforts that seek to influence scientific conduct. However, as I will discuss in the following chapter, this alternative approach to biosecurity not only brings with it new biosecurity interventions, but also new challenges and dilemmas. Although some view a 'risk-aware' synthetic biology community as perhaps the most sustainable 'solution' to a seemingly intractable policy 'problem', others question the appropriateness of making life scientists the 'guardians of sensitive materials' (Zilinskas and Tucker

2002). Moreover, it is unclear to what extent synthetic biologists wish to be made responsible for biosecurity, and how biosecurity practices may influence perceptions of an emerging science and its diverse practitioners.

6.5 Conclusion

In this chapter, I have examined a range of risk management strategies that might be applied (or, in some instances, that have recently begun to be applied) to synthetic biology. These strategies, often referred to as 'top-down' approaches to biosecurity, share a common understanding of what constitutes a 'biosecurity problem', and, in turn, what constitutes a 'biosecurity solution'. Specifically, they each ascribe to the 'classical' biosecurity model, a model premised upon the belief that there exist tangible and intangible artifacts that are, in and of themselves, dangerous things, meriting oversight and control. Under this model, biosecurity depends upon, and is indeed defined by, its capacity to construct 'barriers to access', which are intended to prevent certain (dangerous) persons from gaining access to certain (dangerous) things. As one biodefense scientist described this 'command and control' approach to biosecurity during an interview at the BWC (introduced in Chapter 4): this is a world of "guns, gates, and guards", a world of active monitoring and preventative controls. Albeit a convenient shorthand to describe the classical biosecurity model, biosecurity policies of this kind, as I have shown, are not only differentiated on the basis of their 'technical' capacity to account for and prevent the most urgent dangers, the most pressing threats. They are also differentiated on the basis of their 'practical' capacity – one that is, above all, 'administrative' or 'managerial' in function – to enable these dangers and threats to be organized as risks and made the subject of regulation. In this light, a diverse range of biosecurity controls, ranging from those that seek to restrict access to synthetic genes to those that seek to restrict the publication of research findings describing the *de novo* synthesis of a virus, take on a distinctive rationality, one indicative of a particular 'mentality' of governing. This is the first conclusion that can be drawn from this chapter.

The second conclusion that can be drawn from this chapter is that, while there exist similarities between these risk management strategies, there also exist significant differences. In particular, I have discussed two broad 'families' of biosecurity controls (some of which remain at the inception stage, while others have recently been implemented). The first, exemplified by the *Screening Framework* (DHHS 2010b) for DNA synthesis providers, seeks to restrict access to tangible biotechnologies, including genes, chemical precursors to synthetic DNA, and so on. These interventions are designed to maintain a physical or spatial separation between a select number of physical pathogens (or their constituent parts) and particular kinds of (denied) persons. The second, exemplified by the recent oversight policy on 'dual-use research of concern' (DHHS 2012), seeks to restrict access to various aspects of intangible life science knowledge, including research findings, scientific protocols, and so on. Significantly, this new policy is designed to act upon 'risk objects' that exist 'upstream' of the tangible biotechnologies addressed by the previous family of biosecurity controls. Indeed, it seeks to act upon the very production and dissemination of life science knowledge – restricting or arresting flows of 'dual-use information' – posing a different set of technical challenges and ethical dilemmas; generating a more pronounced tension between national security, on the one hand, and scientific freedom, on the other.

Finally, the third conclusion that can be drawn from this chapter is that, while the classical biosecurity model has proven to be remarkably adaptive – having been applied to the management of diverse 'risk objects' – and while it continues to dominate much biosecurity policy discussion, it is also increasingly contested. Not only do different groups of scientific and technical experts engaged in the design and production of biosecurity interventions of this kind disagree at the level of detail about the content and scope of individual proposals, details which are variously interpreted as more readily 'enabling misuse' or 'inhibiting scientific progress', there also exist growing doubts about the basic assumptions that underpin the classical biosecurity model. Specifically, the traditional framing of biotechnology as a 'technology transfer problem', which assumes that technology possesses 'fixed' functions that can be applied to benevolent or malevolent ends with relative ease, is

increasingly viewed as antithetical to the research experience. Recent scholarship by social scientists, which is gaining growing support among scientific and technical experts engaged in aspects of biosecurity policy, suggests a far more complex, more nuanced, picture of biotechnology. This alternative view of biotechnology suggests that 'tacit knowledge', as well as inherent uncertainties associated with the research process, play an important role in making advanced biotechnology work (or fail). This perspective underlines that bioterrorism might require more than access to a list of ingredients and scientific protocols; and, conversely, that biosecurity might require more than preventing access to science.

7. 'Prudent vigilance': Towards a new 'culture of responsibility'

7.1 Introduction

In the previous chapter, I examined a range of risk management strategies that are intended to restrict access to various aspects of tangible or intangible biotechnology. In keeping with the 'classical' biosecurity model, these strategies are premised upon the assumption that there exist 'intrinsically dangerous' biological artifacts that can (and should) be selectively controlled. However, this approach to biosecurity, I argued, is increasingly contested; not only because it is perceived to be technically demanding to keep 'dangerous tools' out of 'dangerous hands' – a perspective on science that over-simplifies the research experience, treating biotechnology as a 'technology transfer problem' – but also because some believe it may undermine norms of scientific openness and limit scientific progress. In this light, there exists growing interest, I concluded, in an alternative biosecurity model, one that relies less upon controlling access to science (from the 'top-down') and more upon influencing scientific conduct (from the 'bottom-up').

In this chapter, I will examine the second approach to biosecurity, with a view to risk management strategies that are presently being developed and deployed to raise 'biosecurity awareness' among synthetic biologists. Whereas the former set of risk management strategies address the 'dual-use potential' of the science, with little reference to the social actors who might (mis)use the technology, the latter set of risk management strategies takes as its target of intervention the very capacities of synthetic biologists. Ranging from calls on the part of governments and professional organizations for the adoption of professional 'codes' (Rappert 2003) to the development of educational materials designed to encourage university students to reflect on the dilemmas posed by 'dual-use research' (interview with Malcolm Dando, Professor of International Security at the University of Bradford) to the outreach and awareness raising activities of the Federal Bureau of Investigation (FBI) (which provides the primary case study

examined in this chapter), these governance measures are intended to enable synthetic biologists, and life scientists more broadly, to take "a more active role in guarding against misuse" (McLeish and Nightingale 2007, p. 1648).

Part of a wider trend in the life sciences to cultivate a new 'culture of responsibility', these risk management efforts seek to strengthen an existing regulatory regime by way of encouraging greater reliance on scientists to 'govern themselves'. While few argue that this should replace more conventional 'top-down' approaches to regulation, limited 'self-governance' is believed to be an increasingly important component of effective biosecurity policy. Moreover, for some (for example, Kwik et al. 2003), it is perceived to be the most effective means of addressing the 'dual-use problem' in biotechnology, as life scientists are perceived to be in the best position to evaluate the vulnerabilities of their work and to identify possible misapplications. In this context, the role of governmental actors and organizations engaged in aspects of biosecurity policy can be conceptualized as governing through 'indirect action' – promoting specific types of 'self-control' or 'self-management' (Rose 2000). With a view to this ongoing process of 'responsibilization', I will address several questions in this chapter, including: How are synthetic biologists encouraged to be responsible for biosecurity, and why is this perceived to be necessary? What, exactly, constitutes 'responsible life science' in this context, and how does this contrast with existing forms of responsibility in the life sciences? What challenges or resistances are encountered during this process of 'responsibilization', and how might a new 'culture of responsibility' influence how scientists perceive themselves, and how they are perceived by others?

While limited 'self-governance' has been a feature of the life sciences for some time, visible in relation to biosafety practices that have become a routine aspect of institutional science, biosecurity practices are a relatively new addition to the day-to-day responsibilities of life scientists (Reppy 2003). In relation to biosecurity, synthetic biologists (including 'DIY-biologists' and other groups aligned with the 'field' of synthetic biology) are encouraged to consider their research with a view to how it might be 'deliberately misused' and to consider the actions of their colleagues with a view to how they may transgress community norms, posing

'biosecurity risks'. In other words, synthetic biologists are encouraged (to the extent possible) to become 'experts in biosecurity', making routine what has, until recently, been a predominately 'top-down' exercise and the primary jurisdiction of security professionals (ibid.).[119] Indeed, linkages between these formally distinct groups of actors are not only visible in relation to a specific type of 'risk-thinking', one oriented around the subject of 'deliberate misuse', but also in relation to an emerging web of connections that are presently bringing the worlds of science and national security into closer contact in the name of biosecurity.

In this chapter, I will argue that this represents a new – or at least a substantially reconfigured – form of life science 'responsibility', one that is distinct from existing demands for biosafety, and one that is redefining what it means to be a 'responsible life scientist'. Today, and increasingly, I suggest, 'responsible life science' is characterized by the need for scientists to demonstrate that they are at once 'prudent' and 'vigilant' – 'self-disciplined' and 'watchful' – an orientation on risk management that is closely associated with growing concerns about bioterrorism and heightened demands for biosecurity. Whereas 'prudence' implies an underlying responsibility for monitoring one's own conduct in the face of an uncertain future (O'Malley 1992), 'vigilance' implies monitoring the conduct of others in the face of 'deliberate threats'. Being a 'responsible life scientist', in turn, means knowing what biosecurity risks look like, knowing where to look for them, how to measure them, and how to respond to them; it means embracing unfamiliar vocabularies linked with 'terrorism' and 'national security' and engaging with unfamiliar cultures more commonly associated with security and defense.

The case of synthetic biology, which is closely associated with contemporary concerns about bioterrorism, offers unique insight into this emerging web of

---

[119] Reppy, among others (for example, McLeish and Nightingale 2007), refers to these actors as comprising 'the security community'. In opting to use the term, 'security professionals' (see Bigo 2000), my intention is to underline that a wide variety of actors and institutions, in the US alone, participate in aspects of 'national security'. Similarly, as a variety of actors comprise 'the scientific community' (a term that is, again, frequently encountered in the literature), I attempt to differentiate between specific groups of scientists, such as 'synthetic biologists' or 'DIY-biologists'.

connections, as well as the struggles and resistances that accompany this ongoing (it largely remains to be seen to what extent this biosecurity model will result in a 'successful' change in scientific behaviour) process of 'responsibilization'. Although many, including many synthetic biologists (IRGC 2009), view these connections as necessary, and argue that biosecurity awareness raising is not only needed to enhance 'national security', but also to sustain the legitimacy of an emerging science that is perceived to be of particular 'dual-use concern', this approach to risk management is nonetheless contested. On the one hand, there exist doubts about synthetic biologists' capacity to 'police themselves', and questions about the utility of 'self-governance' as a means of preventing the deliberate misuse of modern biology. On the other hand, although supportive of 'self-governance' as an alternative to potentially more restrictive forms of regulation, synthetic biologists are resistant to biosecurity messages that simultaneously cast them as 'biosecurity risks' and as 'strategic partners' in biosecurity – a label some feel is unwarranted and a role others are hesitant to fill. Negotiating these sites of resistance, in turn, represents a formidable challenge to risk management in synthetic biology, and raises new questions about the role of national security in science.

7.2 A new 'Asilomar moment'?

Following the recent controversy surrounding the H5N1 experiments (discussed in the previous chapter), which motivated scientists to declare a temporary moratorium on research projects of this kind (Malakoff and Enserink 2012), many drew a parallel with the Asilomar Conference, connecting this most recent act of 'self-regulation' or 'self-governance' with the self-restraint shown by genetic engineers in 1975 (Berns et al. 2012; Casadevall and Shenk 2012). Some referred to this as a new 'Asilomar moment'. In the words of Stanley Falkow, a microbiology professor and former participant at the Asilomar Conference:

> "[T]he parallels of Asilomar can be applied to the problem facing biomedical science today. We should move forward to establish standardized guidelines, using common sense and scientific creativity. The onus of responsibility falls

> on the individual scientist and involves the education of a new generation of scientists into the social and ethical implications of genetic engineering in a new age of genomics and synthetic biology." (Falkow 2012, p. 1)

Falkow's comments, and the claim that the life sciences are experiencing a new 'Asilomar moment', on the one hand, reaffirm scientists' stated commitment to responsible 'self-governance', underlining the belief that scientists should continue to play a central role in managing the 'risks' engendered by their work. On the other hand, these comments, and the claim that the life sciences are experiencing a new 'Asilomar moment', do not capture how the notion of 'responsibility' in the life sciences has changed – or is beginning to change – in response to a newly visible range of social problems. Today, unlike the earlier case of genetic engineering, calls for responsible 'self-governance' point to a different set of moral and practical obligations, which are tightly coupled with the perceived threat of bioterrorism and growing demands for biosecurity. Embracing multiple governance measures, ranging from prescriptions for biosecurity 'best practices' in institutional research settings (for example, WHO 2006) to codes of ethics that set out aspirational standards by which scientists might judge their conduct (for example, Somerville and Atlas 2005) to a variety of educational resources for scientists to learn more about the nature of 'biosecurity risks' and what they can do to prevent them (for example, NSABB 2011, pp. 2-3), calls for a new 'culture of responsibility' suggest a new orientation on 'responsible life science'. Namely, they convey the growing belief that scientists must not only guard against biotechnology's 'unintended consequences' (biosafety), but also its 'deliberate misuse' (biosecurity).

Although a uniform definition of this new vision of 'responsible life science' cannot be articulated, as multiple actors and organizations are presently engaged in imagining this new 'culture of responsibility', the US Presidential Commission for the Study of Bioethical Issues (PCSBI 2010) expresses a view that is illustrative of the underlying logics of these recommendations. According to the PCSBI (2010), synthetic biologists should adopt a culture of 'prudent vigilance' if their science is to flourish as a secure and sustainable 'scientific enterprise'. Included in this call for responsibility, the PCSBI (ibid, p. 145) points to the need for "'enhanced

watchfulness'", which "requires the scientific community to recognize the varied risks associated with synthetic biology and develop internal processes to identify and respond to potential threats rapidly and effectively." In essence, as I will discuss in further detail, a scientist that is both 'prudent' and 'vigilant' is one that has been sensitized to the threat of bioterrorism and made aware of potential avenues for the 'loss, theft, and potential misuse' of their work, thereby becoming an integral component of a wider biosecurity regime. In brief, it represents an 'ideal type' of life scientist – one capable of playing an active role in biosecurity.

In the context of the laboratory, for example, the WHO (2006, p. 26) states that scientists have a "moral responsibility to ensure that the materials they handle are accounted for and secured" and that "this responsibility lies with the facility managers, the principal investigators and the laboratory staff: all laboratory personnel have a responsibility to take reasonable precautions against theft or misuse." Similarly, the NSABB (2011, p. 2) has encouraged synthetic biologists (and related groups, including do-it-yourself (DIY) biologists), not only to be mindful of their own research, but also "to consider options on how best to minimize the risk that their findings may be misused or misapplied toward malevolent goals." Emphasized in the Fink Report (NRC 2004), widely recognized as having motivated much of the present policy discussion (at least in the US life science policy context) on the role life scientists should play in biosecurity (Atlas 2005b), cultivating a new 'culture of responsibility' will require "that national and international professional societies and related organizations and institutions create programs to educate scientists about the nature of the dual use dilemma in biotechnology and their responsibilities to mitigate its risks" (NRC 2004, p. 4). "We now need to build upon the Asilomar experience", the Fink Committee concludes, "to develop a uniform set of criteria to manage this new set of risks" (ibid, p. 113).

Yet, as the science and technology scholar Judith Reppy (2003, p. 48) rightly argues,[120] these new governance measures are non-trivial, as they demand "nothing less than a cultural shift". Specifically, scientists are encouraged to adopt not only a

[120] See, also, Caduff (2008).

new way of thinking about biological risks, but also a new set of practices, routines and behaviors, which help shape the space within which life science is conducted, and help define what it means to be a 'responsible life scientist'. Moreover, Reppy (ibid.) underlines, a cultural shift of this kind "cannot be imposed from above", but must elicit the cooperation of biologists "and, indeed, the whole network of actors" engaged in the life sciences. For the various organizations and actors engaged in imagining this new 'culture of responsibility', this means devising risk management strategies that foster cooperation – building connections between life scientists and security professionals, two 'communities' that are often said to "speak different languages and face very different incentive structures" (ibid, p. 49). Indeed, as Kwik et al. (2003, p. 32) suggest: "Part of the current lack of awareness stems from the fact that the professional worlds of bioscience and national security do not interact very much or demonstrate a good understanding of each other's concerns". In this light, as the NSABB (2010, p. 12) puts it, if sustained 'biosecurity awareness' is to be achieved, "education efforts and oversight requirements should be tailored to the audience" they are intended to reach. Or, as Filippa Lentzos (2007) suggests, it will be necessary to find "constructive ways of incorporating concern about potential misuse into the professional norms of biological scientists".[121]

Representing both an opportunity and a challenge, connections of this kind contribute to bringing the worlds of 'science' and 'national security' into closer contact, and it is at the intersection of science and national security that this new 'culture of responsibility' is perceived to be possible. Illustrated in Figure 3, security professionals (in this instance represented as a police officer) and scientists (in this instance represented as a public health researcher) are increasingly conceived as 'strategic partners', sharing a common responsibility for guarding against "[i]ntentional misuse" (WHO 2006, p. 26). According to the WHO (ibid.), "those working in biological laboratories have unwittingly become partners sharing in the moral responsibility to ensure that the materials they handle are accounted for and secured, and consequently in the protection of global public health." And, yet, for

[121] See http://www.acronym.org.uk/dd/dd85/85bwc.htm.

many life scientists, at least those working outside of biodefense research settings or other laboratory environments that routinely handle dangerous pathogens (Rappert 2003), the place of national security considerations in science remains unfamiliar, challenging traditional notions of responsibility, which have historically (as I have suggested) centered on the problem of managing the 'unintended consequences' of biological research. For some commentators, including the French biological weapons expert Elisande Nexon (2011, p. 6), this lack of familiarity means that, in the absence of "adequate communication to raise awareness, biosecurity measures may be perceived as an unwelcome and unnecessary constraint … and barely understandable from the point of view of a scientist."

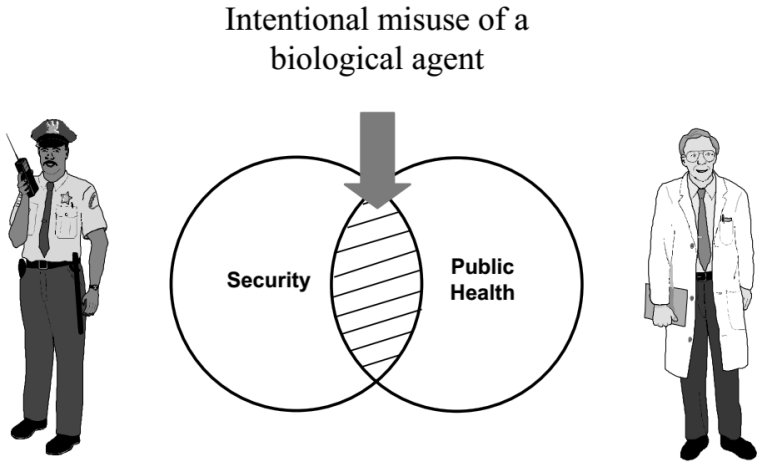

Figure 3: The intersection of security and science (Source: WHO 2006, p. 24).

Thus, the claim that the life sciences are experiencing a new 'Asilomar moment' does not fully capture the extent to which the roles and responsibilities of life scientists are currently being redefined to accommodate biosecurity practices in addition to those of biosafety. In brief, 'responsible life science' in an age of bioterrorism is characterized by a different relationship between scientists and risk. From 'prudence' (characteristic of biosafety) to 'vigilance' (characteristic of biosecurity), scientists are increasingly expected to be both 'self-disciplined' and 'watchful';

encouraged to cooperate with law enforcement and intelligence agencies on matters of 'national security' (Ball 2004). On the one hand, this form of responsibility embraces, and seeks to extend, familiar logics of 'self-regulation', wherein scientists, as 'prudent subjects', are encouraged to "practise and sustain their autonomy by assembling information, materials and practices together into a personalized strategy that identifies and minimizes their exposure to harm" (O'Malley 2000, p. 465). For some time, this has been the mainstay of 'responsible life science', relying on the individual scientist to develop an awareness of hazards in the workplace and to take measures to anticipate and prevent the unintended consequences of their research. On the other hand, these calls for responsibility point to something different, namely, the role of life scientists is increasingly characterized as one of 'self-policing' (see, for example, Ball 2004) rather than 'self-management'.

Nor is this new 'culture of responsibility' precisely comparable to concurrent efforts in research ethics that aim to maintain research standards, and to avert scientific misconduct and academic scandal. Although similarly encouraging scientists to look beyond their own work to consider the actions of their peers and colleagues – in a sense, encouraging scientists to 'police themselves' – risk management efforts of this kind nonetheless draw upon and seek to activate familiar capacities in life scientists. In the case of monitoring potentially fraudulent conduct in life science research, for example, this activity largely depends upon scientific considerations and scientific knowledge. These forms of knowledge and modes of understanding are arguably more easily accessed and mobilized by scientists as a means of auditing and verifying potential transgressions within their 'community'. Biosecurity, in contrast, is said to depend upon cultivating a different set of capacities, ones that are closely aligned with 'national security' considerations and the traditional roles and responsibilities of security professionals.

Before considering in closer detail how this new 'culture of responsibility' is presently being cultivated in the context of synthetic biology, and to what effect, there remains at least one further point of comparison with the Asilomar Conference that bears consideration, and which suggests an enduring feature of 'responsible life science'. Specifically, as the history of science scholar Susan Wright

(1986, p. 615) has shown, the Asilomar Conference was not simply an effort by scientists to mitigate the 'biosafety risks' posed by genetic engineering, but also an effort to protect "biomedical research from external regulation." In other words, it was not only an attempt to determine the best means of *doing* genetic engineering responsibly, but also a means of *demonstrating* that genetic engineers could be responsible. By taking it upon themselves to become their own risk managers, a view that is currently supported by many synthetic biologists (see, for example, IRGC 2009), genetic engineers sought to free themselves from other (potentially more restrictive) forms of oversight and regulation. In this light, the recent research moratorium called by H5N1 scientists,[122] often favorably described as a new 'Asilomar moment', can equally be understood as an effort by scientists to forestall "heavy-handed government regulation" (Malakoff and Enserink 2012).

Therefore, although the roles and responsibilities of life scientists are presently being redefined in response to growing concerns about bioterrorism and heightened demands for biosecurity, the perceived need to demonstrate practical action in the face of uncertain risks remains much the same. Although rarely featuring in policy-accounts of the Asilomar Conference, this meeting (and the more recent moratorium on H5N1 research, albeit with a view to biosecurity, as opposed to biosafety) was instrumental in more than one sense. It served as a means of enhancing biosafety, and it served as a means of sheltering an emerging biotechnology from potentially more restrictive forms of regulation. In both instances, these objectives were facilitated by the call for 'prudent self-regulation'. This perspective on the Asilomar Conference, I suggest, is equally indicative of the 'Asilomar experience', and equally characteristic of current calls for 'self-governance' in synthetic biology. Yet, as the preceding discussion suggests, scientists' willingness to participate in biosecurity – a practice that envisions scientists as not only their own risk managers, but also their own police – is more tenuous than that of biosafety, raising new questions and dilemmas.

---

[122] The moratorium, which was announced in a letter signed by 39 leading influenza researchers on 20 January 2012, has now come to an end, after approximately one year. By some accounts, this marks the end of the H5N1 controversy (Malakoff 2013).

7.3 Cultivating a new 'culture of responsibility'

In recent years, I have suggested, there has been a growing emphasis on establishing a new 'culture of responsibility'. Justified in part by heightened concerns about bioterrorism, and in part by a perceived lack of biosecurity awareness among life scientists, including synthetic biologists (Kelle 2007), as well as growing doubts about the efficacy and desirability of restricting access to 'dual-use biotechnology' (Chapter 6), biosecurity education and awareness raising has come to be increasingly favored as a practical means of engaging scientists to play a more active role in countering the threat of 'deliberate misuse'. As the NSABB (2011, p. 2) suggests in relation to its so-called "strategic plan on outreach to all stakeholder communities about dual use research … a successful system of oversight depends on the ability of researchers to recognize the dual use potential of their work and to consider options on how best to minimize the risk that their findings may be misused or misapplied toward malevolent goals." To achieve this objective, the NSABB (2010, p. 9) suggests, "outreach and educations [*sic*] strategies" must be developed "that target relevant communities." In the case of synthetic biology, these include: "researchers who are a) not subject to federal biosafety and biosecurity requirements (e.g., private sector), b) not formally affiliated with universities or research institutions, and c) students (at all levels)" (ibid, p. 14).

In this section, drawing on interviews with (amateur) synthetic biologists, law enforcement agents, and biological weapons experts interviewed in the context of the BWC, as well as data from the biosecurity policy literature, I will consider how biosecurity awareness raising activities (especially those of the FBI in their ongoing engagement with DIY-biologists) attempt to enable synthetic biologists to become active contributors to biosecurity. More precisely, I will consider how biosecurity awareness raising activities seek to enable a particular kind of 'responsible life scientist' (one who is both 'prudent' and 'vigilant') and how a new 'culture of responsibility' is beginning to emerge, and to what effect. Taken together, I will argue, although this approach to biosecurity is viewed by many (including many

synthetic biologists) as a promising and efficient means of countering the threat of bioterrorism, as well as sustaining the legitimacy of an emerging science that is closely associated with 'dual-use concerns', there remain diverging opinions about the role synthetic biologists should play in biosecurity. Moreover, there exists an uneasy relationship between the worlds of science and national security, complicating functional partnerships between scientists and security professionals, and raising new questions about the role of security in science.

Much like the risk management strategies discussed in the previous chapter (and the case of the DNA synthesis industry, Chapter 5), which I argued are intended to 'manage' or 'organize' the material and informational elements that makeup synthetic biology in pursuit of a secure and sustainable 'scientific enterprise', this research suggests that biosecurity awareness raising activities directed at synthetic biologists presuppose that it is possible to reform human beings, to reshape their attributes and to direct their capacities towards productive ends (Miller and Rose 1990; Dean 1999; Rose 2000). From 'administering things' to 'administrating persons', the same logics of 'manageability' that are applied to 'synthetic genes' and 'dual-use research' are equally apparent in relation to biosecurity 'outreach and education strategies' (NSABB 2010) directed at influencing the conduct of life scientists. However, unlike the risk management strategies discussed in previous chapters, which primarily address the organization and management of inanimate 'risk objects', synthetic biologists are free to interpret and to resist biosecurity messages, and, thus, these messages must be made understandable and acceptable to scientists on their own terms. This, in turn, requires successfully tailoring biosecurity messages to the life science audiences they are intended to reach.

From a regulatory standpoint, this research also suggests that limited 'self-governance', as a mode of regulation, is increasingly viewed as an efficient means of allocating responsibility and managing risk. As Bounds (2010) suggests:

> "The careful allocation of responsibility for risk management has the potential to produce greater economic benefits by allowing risks to be managed at the level of society where it will be most effective. This can include reducing unnecessary reliance on government involvement in individual's lives,

> thereby building a more resilient society and allowing opportunities for adaptive behaviour." (Bounds 2010, p. 25)

Or, as Kwik et al. (2003, p. 33) argue in relation to the life sciences, an effective "governance system for bioscience should engage the practitioners of science in an integrated management of biosecurity concerns." This is because "scientists themselves", they suggest, "best understand the ways in which the craft and business of biological science might be most efficiently governed" (ibid.).

Before proceeding, two qualifications are also necessary. First, although opinions differ as to the role life scientists should play in 'policing science', and who should ultimately be accountable for biosecurity, 'self-governance', as a mode of regulation, is by no means perceived to be undesirable from the standpoint of synthetic biologists. "Within the synthetic biology community," the IRGC (2009, p. 10, citing Campos 2009) suggests, "there is considerable support for approaches to oversight that rely on measures developed and implemented by the community itself". Indeed, by as early as 2006, "[a]t the Second International Meeting on Synthetic Biology (SynBio 2.0) in Berkeley … participants put forward a declaration on the governance of the field, which focused on biosecurity issues and emphasised self-regulation" (ibid.). Similarly, synthetic biologists are not the passive recipients of biosecurity awareness raising efforts coordinated on behalf of government authorities. On the contrary, it is equally perceived to be in the interests of synthetic biologists to cultivate their 'biosecurity awareness'. At the same time, to what extent this reflects an advanced concern about the 'biosecurity implications' of their work, versus a desire to avoid more intrusive government oversight and regulation, and to avoid familiar lessons (notably, GM crops) associated with minimal societal engagement on matters of public concern, is open to question (ibid.).

Second, it is important to underline that there exist further examples of 'biosecurity awareness raising' that I do not attempt to address in this section. Moreover, while each of these efforts ostensibly share an overarching commitment to enabling scientists to play a more active role in biosecurity, they do so by a variety of means, reflecting different institutional commitments and priorities, contributing to somewhat different understandings of what should count as

'appropriate' self-governance. For example, in the case of 'codes of conduct', which represent one method of raising biosecurity awareness that have received "renewed interest … as a means of mobilizing the scientific community across many organizations and countries", Rappert (2003, p. 167) notes that there exist varying competing opinions on: "who should devise codes, whether they should be voluntary, what purpose they might serve," as well as "what issues they should cover, by what mechanisms they could be agreed, whether a new code is necessary or existing ones should be augmented, and whether there should be a single universal code or varied local ones." In this light, it is apparent that, while the specific awareness raising activities discussed in this section highlight a number of key biosecurity messages that can be used to help characterize ongoing efforts to establish a 'risk-aware' life science community, there is neither a uniform vision for how this might be achieved, nor a consensus view of what exactly a 'community' of this sort might look like. This is because 'biosecurity awareness raising' takes multiple forms and is the product of diverse actors and organizations, ranging from government agencies to professional organizations, biotechnology industries to academia. Moreover, "life scientists" (despite frequent portrayals to the contrary) "are a highly heterogeneous population" (Relman 2010, p. 276).

7.3.1 'Building Bridges Around Building Genomes': Getting to know your 'local WMD Coordinator'

On 4-5 August 2009, the FBI hosted a conference in San Francisco entitled 'Building Bridges Around Building Genomes'. Its goal was to bring together "science and security communities to come to an understanding to promote a culture of responsibility"[123] and to consider steps that might be taken to ensure that DNA synthesis technology is used only for beneficial applications. For Special Agent You, of the FBI's Weapons of Mass Destruction (WMD) Directorate, the Building Bridges conference marked an important turning point in the FBI's engagement with

[123] Edward You, cited in Lempinen (2011), available at: http://www.aaas.org/news/fbi-aaas-collaborate-ambitious-outreach-biotech-researchers-and-diy-biologists.

(amateur) synthetic biologists. During my interview with Agent You, a leading figure in the FBI's outreach and awareness raising activities with life scientists, he recalled that the conference (and other initiatives of this kind) signaled a "paradigm shift because there's always been a rift, or a gap of mistrust, between academia and law enforcement", whereas now "we're basically acting as a resource, trying to establish a partnership, and academia is very receptive, and want more of this engagement." For Jason Bobe, co-founder of DIYbio,[124] and a participant at the Building Bridges conference, this meeting was equally significant, but for somewhat different reasons. According to Bobe, the Building Bridges conference marked the beginning of a constructive – yet, at times, uneasy – engagement between "DIYbio and law enforcement", one that has seen growing interest in amateur biology, and its indirect pairing with the themes of "biosecurity" and "bioterrorism".

While the Building Bridges conference represents only one site of engagement between life scientists and security professionals, it is, I suggest, illustrative of an ongoing process of 'responsibilization' that sees the worlds of science and national security interacting in new ways in the name of biosecurity. For Agent You, and for other experts interviewed for my research (David Franz; Piers Millett; Christopher Park; Dana Perkins; Amy Smithson), this engagement is perceived to be necessary because synthetic biology (and amateur biology, as a demonstration of 'democratized' science) calls into question the foundational logics of 'biosecurity', a defensive practice premised upon keeping 'dangerous tools' out of 'dangerous hands' (Chapter 4). In light of broad based capabilities in the life sciences, and an expanding portfolio of equipment, information and research techniques that have been identified as 'biosecurity risks' to be 'managed', a 'command and control' approach to biosecurity is viewed as increasingly impractical, and possibly 'bad for science' (Chapter 6). For many, this suggests a need for a new approach to biosecurity, one that relies less on controlling access to science, and more on enabling scientists to become their own 'risk managers', and, in many ways, their own 'police'. According to Agent You:

[124] See http://diybio.org/.

> "The most effective method [of biosecurity] is to engage the life science community, so they can police themselves … so they can be in a position to identify not only the risks and vulnerabilities, but also potential nefarious activity, and then to be in a position to report it to the appropriate parties, which includes the FBI, of course." (Edward You)

From the perspective of DIY-biologists like Jason Bobe and McKenzie Cowell, Bobe's colleague and co-founder of DIYbio, cooperating with law enforcement and becoming active participants in biosecurity is equally perceived to be important, but not strictly because they feel they are best suited to the task of identifying the 'risks' and 'vulnerabilities' associated with amateur biology. On the one hand, they acknowledge there exist concerns about DIY-biology's "potential for deliberate misuse", and express a willingness to participate in biosecurity initiatives (Jason Bobe and McKenzie Cowell interviews). On the other hand, they are "very conscious of law enforcement's interest in DIYbio", which leads them to believe that the sustainability of the "amateur biology movement" partially depends upon demonstrating a "culture of safety and security" (Jason Bobe and McKenzie Cowell interviews). In Bobe's opinion, biosecurity awareness within the DIYbio community, and being seen to participate in biosecurity initiatives, is essential because "DIYbio has been cast as such a controversial, high-risk activity for society", and there is "a real worry" that a perceived lack of responsibility (or, in the worst case, a "biosecurity incident") on the part of amateur biologists might generate a "knee-jerk reaction" that could "set back the whole field of synthetic biology."

In this light, the emerging 'partnership' between the FBI and DIYbio reveals itself to be one based upon a sense of reciprocity, but one that is understood somewhat differently by their respective spokespersons. For Agent You, "it's about recognizing that we all have a role to play, and that we are all dependent upon one another, and that we all need to work together to address these risks." This, in turn, has motivated the FBI to reach out to local DIYbio 'chapters' across the US, as well as to undergraduate teams at the annual International Genetically Engineered Machine

(iGEM) Competition[125] and to academic institutions across the country, to "build bridges" between scientists and local FBI field agents ("WMD Coordinators")[126] in an effort to "educate students about responsible conduct … priming that next generation of synthetic biology practitioners to be able to address these issues in the future." For Agent You, the FBI's WMD Coordinators are the "educators and also the bridge lines, so if there was ever an incident of some kind, they would be the bridge between the local-level and the headquarters-level, where I sit."

Whereas, for Jason Bobe, engaging with law enforcement is not only about mitigating 'biosecurity risks', but also limiting the controversy surrounding amateur biology activity. According to Bobe, if this means, "getting to know our local WMD Coordinator, 'Dan', that's fine". "The problem", he explained,

> "is that at the end of the day, their job is still to enforce *the law*. And if they come in [to a DIYbio community lab] and see that somebody is mailing— you know, if the lab isn't up to code or something – if something breaks *the law* – it just causes concern among community members, and they may be less willing to participate in an open and transparent manner." (Jason Bobe)

As Bobe's account suggests, although willing to meet with their 'local WMD Coordinator', in part because this is perceived to provide the necessary assurances that their local DIYbio group is not causing harm, some 'community members' continue to view law enforcement agents as outsiders and their visits can generate 'concern'. Because, as Bobe suggests, their WMD Coordinator's 'job' is 'to enforce the law', he worries that some DIY-biologists may feel "they are putting themselves in a legal liability situation by asking for help." Consequently, Bobe believes "there's some negotiation that needs to happen here [with law enforcement] to make it

---

[125] See http://igem.org/Main_Page.

[126] Agent You offered further background on the FBI's WMD Coordinators: "In each of our 56 field offices across the US, there's one Special Agent who's designated the WMD Coordinator for their region. They receive training above and beyond their training as an Investigator. They're educated about CBRN [chemical, biological, radiological, and nuclear] issues. And they are the point of contact for, and they liaise with, industry, academia, even the amateur biology groups (if they happen to be in their area)."

acceptable for individuals; to not feel threatened by doing these activities, and so there's a whole lot of work that needs to go into that."

In many ways, I suggest, the Building Bridges conference, and the FBI's ongoing engagement with DIYbio, represents a test case for a larger project or program that aims to bring together life science and security 'communities' to jointly address the problem of 'deliberate misuse'. On a larger scale, there exist a growing number of policy initiatives calling for cooperation between life scientists and security professionals, emphasizing the need for "Creating New Partnerships Between the Science and Security Communities" (NRC 2007, p. 81)[127] and for "'joined-up' thinking across all responsible sectors, namely government, the scientific community and the biotechnology and pharmaceutical industries" (ICRC 2004)[128] to address the threat of bioterrorism. Whether in the form of interdisciplinary working groups (for example, NRC 2007) or joint policy papers (for example, Bügl et al. 2007), each site of engagement between life scientists and security professionals suggests a promising opportunity for collaboration. At the same time, as the FBI-DIYbio case suggests, there exists an underlying tension between these groups, each of which is perceived to possess different cultural frames, professional interests, expectations and concerns, which puts science and security communities, it has been suggested, at risk of "'talking past each other'" (NRC 2007, p. 77). From the perspective of the FBI, and for others in favor of encouraging greater reliance on 'self-management' or 'self-policing' in the life sciences, scientists are viewed as an invaluable resource, constituting "a distributed, self-reinforcing, and adaptive protection system" (Relman 2010, p. 277) capable of detecting and (it is hoped) preempting potential 'nefarious activity'.

For life scientists, their engagement with law enforcement and security communities is at once a reflection of their concern about the 'primary' risks that might arise in the context of their research and the 'secondary' or 'reputational'

---

[127] See National Research Council (NRC 2007, pp. 77-84), 'Partnerships for Science and Security', available at: http://www.nap.edu/openbook.php?record_id=12013&page=77.
[128] See International Committee of the Red Cross (ICRC 2004), 'Responsibilities of Actors in the Life Sciences to Prevent Hostile Use', available at: http://www.icrc.org/eng/resources/documents/misc/5vdjlw.htm.

risks that might arise from a perceived failure to act responsibly (Power et al. 2009). In the case of DIYbio, this means that, irrespective of whether their ongoing collaboration with law enforcement is perceived to be ideal, it is nonetheless perceived to be important to demonstrate their willingness to participate in biosecurity initiatives – a view that would appear to be shared by the wider 'synthetic biology community', which is frequently noted for its commitment to 'upstream engagement' (Lentzos 2009). Indeed, it is evident that many life scientists believe that, "the best way to keep the pursuit of knowledge open and free is for researchers to exercise a demonstrable sense of responsibility" (Nature 2006, p. 715), and being a 'responsible life scientist', especially in post-9/11 America, can, quite arguably, no longer be separated from participating in biosecurity.

In this light, the outreach and awareness raising activities of the FBI with DIYbio, which have been among the most vigorous sites of biosecurity engagement with (amateur) synthetic biologists in the United States, take on a strategic coherence. From the perspective of both parties, there are perceived to be mutual benefits to cooperation. At the same time, this cooperation is not without its own challenges and dilemmas, especially from the perspective of DIY-biologists, who are, if indirectly, framed as both 'allies' and 'potential threats'. The FBI-DIYbio case can equally be understood as one manifestation of a more general trend that is bringing the worlds of science and national security into closer contact in pursuit of a 'secure' and 'sustainable' science. Yet, whether 'partnerships' of this kind will flourish remains open to question. For Agent You, the 'gap of mistrust' between scientists and law enforcement appears to be closing, whereas DIY-biologists express a more ambivalent attitude. For the time being, it would appear that DIY-biologists view their partnership with the FBI as one that is no less a matter of self-preservation, as it is a matter of shared conviction. Yet, according to McKenzie Cowell, despite this evident tension, "both sides benefit (for now) from that relationship."

7.3.2 Making scientists 'experts in biosecurity'

The challenge of building a sense of mutual trust between life science and security communities is interconnected with the broader challenge of cultivating a new 'culture of responsibility'. In the case of the FBI's engagement with DIYbio, and across multiple sites of ongoing biosecurity awareness raising, a variety of educational resources, incentives and penalties (for example, in the form of legal requirements under the Select Agent Regulations) are presently being mobilized to motivate and enable life scientists to become (to the extent possible) their own 'experts in biosecurity'. Embracing a distinctive form of 'advanced liberal' government, one that is characterized by "steering and regulating rather than rowing and providing" (Rose 2000, p. 324), international organizations, federal agencies, scientific institutions, and others, are presently developing risk management strategies that are intended to enable life scientists to play a more active role in biosecurity. In the following, continuing to draw upon the FBI's outreach and awareness raising activities with (amateur) synthetic biologists, but with a view to the wider biosecurity policy debate, I will highlight the manner in which this new form of 'responsible life science' is presently being pursued.

From the perspective of Agent You, among others (for example, Kwik et al. 2003), life scientists are perceived to be in the best position to identify biosecurity risks that might arise in the context of their work, which should then, according to Agent You, be reported to the FBI or other "appropriate parties". In this light, beyond the challenge of creating channels of communication between WMD Coordinators and (amateur) synthetic biologists, there is perceived to exist a further challenge of ensuring that scientists are made aware of how to identify, assess, manage and communicate risks of this kind. As Agent You described in relation to one aspect of the FBI's outreach and awareness raising activities: at the outset of presentations to "undergraduate students, all the way up to university leadership", "I like to quote Spiderman: 'With great power, comes great responsibility'". What follows – both in relation to Agent You's didactic PowerPoint presentations (which I have had the opportunity to see on two occasions) and in relation to an ongoing

process of 'responsibilization' more generally – are a series of message points that endeavor to communicate what form this 'responsibility' might take.

Although a uniform approach to biosecurity awareness raising does not exist, as evidenced by an array of educational resources, codes of conduct, appeals to norms, and alike, which have recently come to populate the life science policy literature, the general aim of these activities, I suggest, is to establish a degree of situational awareness among life scientists, enabling them to become (to the extent possible) their own 'experts in biosecurity'. For example, at the Building Bridges conference, introduced above, the FBI ran a "tabletop exercise" that, according to Agent You, aimed at "instilling that nugget of knowledge about biosecurity issues, so that scientists can consider these questions and identify these issues later on in their careers." Agent You's description of this tabletop exercise helps shed light on the kinds questions that scientists are encouraged to consider:

> "We provided some hypothetical scenarios. For example, if someone tried to illicitly gain access to sequences or dangerous pathogens or toxins, or if someone was showing suspicious behavior within the community, or if someone noticed that someone was trying to exploit them for information, and so on. We provided them with a story line, and asked: 'What would you do?' 'How would you react?' 'Who would you notify?' And it's very enlightening for the participants to realize that: 'You know what, these are possible threats, and if I do encounter them, who do I need to contact? What actions can I take?'" (Edward You)

According to Agent You, the FBI uses variations of this tabletop exercise at meetings and conferences across the US, using "scenario stories" in combination with "a series of didactic presentations" to help give scientists "a law enforcement perspective on biosecurity … introducing them to another world, basically."

In addition to providing a platform for engagement between scientists and security professionals, outreach and awareness raising activities of this kind, as Agent You's account suggests, are intended to introduce scientists to 'another world'. This 'other world' is the world of 'law enforcement' and 'national security', professional domains characterized by a different way of thinking about laboratory

equipment, scientific knowledge, and the day-to-day activities of life scientists. According to David Relman (2010, p. 275), a microbiologist and active contributor to biosecurity policy discussions in the US, "the life-sciences research and national security communities" have "widely disparate cultures and styles", each having "a different understanding of the global life-sciences landscape" and use "different criteria for defining and interpreting incongruities in this landscape". Consequently, Relman and others argue that raising biosecurity awareness among life scientists ultimately requires teaching them to think differently about their work and about the risks that might arise in the course of their research activities. In the case of the FBI's tabletop exercise, for example, scientists are encouraged to consider a range of scenarios that may be unfamiliar to them, including the possibility that someone might attempt to "illicitly gain access to sequences or dangerous pathogens or toxins". They are encouraged to be mindful of "suspicious behavior within their community", and to be aware of whom to contact in the event that biosecurity risks should be identified. These are among the many contingencies, "possible threats", and practical actions synthetic biologists are encouraged to consider in relation to their new responsibilities as 'strategic partners' in biosecurity.

Awareness raising activities of this kind, in brief, can be thought of as efforts to teach scientists to think more like security professionals, encouraging them to adopt a new perspective on biological risks and their responsibilities as life scientists. As Agent You expressed on several occasions, the FBI's approach to awareness raising is about "encouraging scientists to think about how these technologies could be used for nefarious purposes"; about finding ways to "prevent the exploitation or the subversion of the technology for nefarious use"; and about "providing scientists with the situational awareness that there are these potential risks and vulnerabilities, and possible threats." Others interviewed for my research, including Amy Smithson, a chemical and biological weapons expert who regularly conducts outreach and awareness raising activities with scientists, argue that it is important to teach scientists to think about "the potential downsides of an experiment", which can help "start to change the laboratory environment."

Further details on 'responsible life science' are visible in the form of a variety of educational resources, which are available to life scientists through an assortment of mediums. For example, a recent publication by the NSABB (2011, p. 3) describes YouTube videos, brochures and DVDs that have been designed to offer "a conceptual introduction to the dual use research issue", and which have been made available to scientists online, at presentations and poster sessions. One video, hosted on the National Institutes of Health website, entitled "Dual Use Research – A Dialogue",[129] features prominent life scientists, public health officials, medical doctors, and biological weapons experts discussing the nature of 'dual-use risks' and the various actions that scientists might take to mitigate these risks. The video is divided into three parts, including sections on: "What is dual use research?" "What can be done?" and "How should we prepare for the future?" In this video, scientists are reminded that: "We have a responsibility, not only to our personal research, but to the scientific community … and to the communities we live in."

Other experts interviewed for my research recommend more intensive forms of education, introducing concepts such as "ethics", "membership", "enlightened leadership", "openness" and "trust". For example, according to Amy Smithson, she believes scientists should receive

> "ethical instruction, raising awareness of their membership in mankind, and the fact that they're part of the human race and it's not all about 'Do I publish or perish?' or 'Do I beat my competition to discovery 'x'?' When you are dealing with these areas of science, which have the potential to devastate the planet, I think there are larger responsibilities at hand, and it ought to be mandatory to have that type of instruction." (Amy Smithson)

In another interview, David Franz, a senior biodefense scientist and former member of the Fink Committee (NRC 2006), expressed that he believes that, "while there are places for guns, gates and guards", the best mechanism of risk management in the life sciences is through "soft power" and "hearts and minds". According to Franz, biosecurity awareness raising should be about encouraging:

[129] Available at: http://oba.od.nih.gov/biosecurity/biosecurity.html.

"Enlightened leadership, quality research, vision, responsibility, honesty and openness, full and total access … [and] building a culture of trust."

Irrespective of the content and scope of the biosecurity guidance offered to life scientists, this guidance is, necessarily, non-exhaustive. Instead, it functions as a primer, encouraging a new way of thinking about biological risks, and providing an introductory vocabulary for talking about biosecurity. As Agent You commented in relation to the FBI's tabletop exercise, for example, the primary aim of awareness raising activities of this kind is "to prompt discussion", "to get everyone talking", to provide "that nugget of knowledge about biosecurity issues". It is, in turn, expected that scientists will carry this knowledge forward, translating biosecurity guidance into practical action, while simultaneously remaining engaged with, and seeking support from, a wider 'security community' (of which, it would seem, they are increasingly a part). According to Gretchen Lorenzi, an intelligence analyst with the FBI, she believes "that the science community 'has an ability to deal with and take responsibility for its own vulnerabilities, but … the FBI can be an asset in that fight'" (cited in NRC 2007, p. 83). Or, as Dana Perkins, a public health official and biological weapons expert who conducts outreach and awareness raising activities with amateur biologists at DIYbio community labs, explained during an interview: "[community labs] can ask for support from a federal agency like the FBI. That's up to them. That is their due diligence. We basically put the ball in their court, so they will have to decide what constitutes their due diligence."

These accounts illustrate that (amateur) synthetic biologists are, to a large extent, made to enact their own form of 'responsible life science', where biosecurity guidance serves as much to activate scientists' individual capacities to think and act responsibly, as it does to educate them on how to be responsible. For example, in the case of the FBI's tabletop exercise, the FBI first attempts to educate and orient scientists to think about their work with a view to biosecurity, and, second, encourages scientists to interpret the best course of action in light of the biosecurity

guidance they have received.[130] In essence, this is the underlying principle of governance strategies that seek to enable individuals, families and communities to play a more active role in their own self-management, and who are, with limited guidance, intended to provide for their own security. As Rose (2000, p. 327) suggests, this form of government can be characterized by "the metaphor of the facilitating state, the state as partner and animator rather than provider and manager." In the case of the FBI's awareness raising activities with (amateur) synthetic biologists, FBI agents describe themselves as 'educators' and 'facilitators' – or as 'assets' in the fight against bioterrorism (NRC 2007, p. 83) – while scientists are encouraged to take a leading role in the management of biosecurity risks.

This approach to 'responsible life science', one that "depends on the scientific community's will, capacity, and commitment to regulate itself" (Maurer and Zoloth 2007, p. 17), is further reinforced by calls for scientists to support the efforts of security professionals by way of providing information and guidance that might improve their own capacity to mitigate potential biosecurity risks. The notion of scientists educating security experts is clearly visible in relation to two comments made by Agent You. In the first instance, Agent You emphasizes that synthetic biologists can educate the FBI on "the state-of-the-art" in synthetic biology and "what they see coming over the horizon", thereby equipping the FBI with the necessary knowledge to "develop the proper security measures":

> "It's a two-way street. It's not just about us preaching to the communities about security, but it's a two-way educational process, where we learn more about the field, what the state-of-the-art is, what they see coming over the horizon, and that equips us with the knowledge about how we can best prepare for it and ensure that we develop the proper security measures." (Edward You)

[130] As discussed in Chapter 5, the Department of Health and Human Services' (DHHS 2010b) *Screening Framework* serves a similar function, providing 'screeners' with a more or less structured procedure for conducting biosecurity risk assessments, which is then adapted according to a screener's experience and intuition.

In the second instance, Agent You emphasizes that synthetic biologists can also "assist" the FBI in conducting biosecurity risk assessments, provided they have developed the necessary "situational awareness":

> "If we've engendered their trust, provided them with the situational awareness that there are these potential risks and vulnerabilities, and possible threats … the practitioners themselves can then engage us in law enforcement, educate us, and help us define what those risks potentially could be and help assist us in the assessment." (Edward You)

The notion of scientists assisting security experts, not only on matters of science, but also on matters of security is, in many ways, an inversion of the typical allocation of responsibilities that one might expect of a security regime.

Taken a step further, Piers Millett, a senior administrator for the BWC, imagines a future where the "security community" plays a minimal role in 'policing science'. According to Millett:

> "If we can influence the behavior of the practitioners … we've suddenly got a resource we can use. More importantly, we end up with an appreciation of [biosecurity] that goes across everywhere. It's no longer just a security issue for the security community to deal with. This becomes an issue for the synthetic biology community to deal with and hopefully people like me won't be needed in five years time because this is something they're doing off their own back, completely unaided." (Piers Millett)

The extent to which this level of self-sufficiency will come to fruition is, of course, uncertain. What is clear, however, is that some security professionals desire (and anticipate) a larger security role for scientists.

However, there are others who are critical of this vision of responsibility, arguing that synthetic biologists (or life scientists by any other name) neither possess the moral authority nor the technical competency to take responsibility for anticipating and preventing acts of bioterrorism (for example, ETC Group 2007; Selgelid 2007, 2009; Steinbruner et al. 2007). In relation to the question of scientists' technical competency, the bioethicist Michael J. Selgelid argues that:

> "Scientists might be best able to recognize a discovery's scientific or technical implications for the making of particular biological weapons, but they have no special expertise to determine the identity, abilities, or intentions of potential bioterrorists. And scientists have no special expertise to assess what the *security* – as opposed to health – implications of attack [*sic*] with particular biological weapons would be." (2007, p. 41)

In addition to this perceived lack of expertise, Selgelid (ibid, p. 41) questions scientists' objectivity to make security decisions that could diminish scientific freedom: "just as governmental officials are likely to have values biased in favor of security over the promotion of science, scientists and science editors are likely to be biased in favor of the promotion of science over security." Moreover, for Selgelid, and for other bioethicists who have chosen to address the subject of biosecurity, the 'dual-use dilemma' is above all a question demanding 'ethical' attention, and ethicists (neither scientists nor security professionals) are said to be best suited to this task (Selgelid 2007, 2009; Douglas and Savulescu 2010).

Civil society organizations, such as the ETC Group (2007), have been particularly critical of proposals for 'self-governance' in synthetic biology, asserting that the 'implications' of the science – including social and ethical considerations beyond those of biosecurity – are too great to leave in the hands of scientists, who they believe are primarily interested in minimal oversight and regulation. In reference to the legacy of the Asilomar Conference, the ETC Group rejects calls for "'Asilomar 2.0'" (ibid, p. 47) and is unwilling to accept the view: "Trust us, we're experts" (ibid, p. 46). The authors argue that, just as "Asilomar participants focused narrowly on biosafety issues", synthetic biologists wish to focus on a finite set of issues related to biosecurity at the expense of broader social debate (ibid.). "If a small circle of synthetic biologists get their way," they claim, "governance of extreme genetic engineering will be left entirely in their hands" (ibid.).

Yet, for their part, synthetic biologists have expressed ambivalent attitudes about 'policing themselves'. Beyond the fact that 'self-governance' is generally viewed as preferable to potentially more restrictive forms of oversight and regulation, it is not clear that scientists wish to take primary responsibility (or at

least be held accountable) for biosecurity. On the one hand, they assert their shared concern about biosecurity risks, and a common interest in preventing the deliberate misuse of their science. On the other hand, they resist the notion that they should be held personally accountable (and possibly liable) for biosecurity. For example, in an article entitled 'DNA synthesis and biological security' (a joint policy paper published in *Nature Biotechnology*, which included the prominent synthetic biologists George Church and Drew Endy among its lead authors), Bügl et al. (2007, p. 628) argue that, although scientists and public health agencies have an important role to play in assisting law enforcement, "ultimately, it is the specific responsibility of law enforcement authorities to protect individuals and communities against threats that may arise through the misuse of this promising technology." As Rappert (2003) points out, this ambivalent stance towards responsibility is not uncommon among scientists and other professionals when confronted with the issue of 'accountability', a subject that necessarily goes hand-in-hand with calls for 'responsible self-governance'. In reference to Cunningham-Burley and Kerr's (1999) work on genetics and social responsibility, Rappert (ibid, p. 305) notes: "Professional responsibilities were defined so to make researchers vital for addressing social problems but ultimately not responsible for them."

In light of these underlying tensions, it is unclear precisely what configuration of 'responsibility' will ultimately emerge in synthetic biology, and to what extent synthetic biologists are prepared – both in terms of their technical competencies and their willingness – to 'police themselves'. Yet, as I will discuss now, there are at least signs to suggest that, within some segments of the 'synthetic biology community', biosecurity awareness raising efforts have begun to motivate a new orientation on 'self-governance', one that favors a culture of 'prudent vigilance'. Moreover, while this development suggests new opportunities for science and security, it also holds the possibility of unforeseen consequences, as scientists are increasingly represented as not only their own 'risk managers', but also their own 'police'; made to negotiate a policy landscape that portrays them, at least tacitly, as 'biosecurity risks' and as 'strategic partners' in biosecurity.

7.3.3 Scientists who 'police themselves'

If the purpose of biosecurity awareness raising, as a number of the preceding accounts suggest, is to "change the laboratory environment" (Amy Smithson), to "influence the behavior of practitioners" (Piers Millett), to encourage biologists to think about how their research "could be used for nefarious purposes" (Edward You), to enable scientists (to the extent possible) to become their own 'experts in biosecurity', then, to some extent, a new 'culture of responsibility' has begun to emerge among some life science communities. Already, according to Agent You, there are promising signs that a significant level of biosecurity awareness has been established among DIY-biologists as a result of awareness raising activities initiated by the FBI. In reference to Genspace,[131] a DIYbio community lab in New York City that has been the target of some of these initiatives, Agent You explained:

> "They're kind of the poster child, and hopefully they're developing best practices that can be conveyed to other future community labs that come online across the US, because they're, for all intents and purposes, the *leaders* now – the local amateur groups will probably be looking to them as to how to develop their own community spaces." (Edward You)

Agent You's enthusiasm about Genspace's leadership, and their potential interest in developing their own biosecurity 'best practices', although not necessarily representative of wider biosecurity awareness raising projects in synthetic biology and the life sciences more broadly, is a testament to an emerging 'culture of responsibility' that has, by some accounts, advanced to the stage that scientists are beginning to be viewed as their own 'educators' in biosecurity.

Similarly, recent outreach efforts by the FBI (Edward You) and the BWC's Implementation Support Unit (ISU) (Piers Millett) at the annual iGEM Competition have, by some accounts, begun to influence the research process. In an effort to raise biosecurity awareness among student teams, the FBI and the ISU have held workshops covering "dual-use issues, dual-use research of concern, and responsible research", generating discussions that were, according to Agent You, "phenomenal".

[131] See http://genspace.org/.

Moreover, as a component of the iGEM Competition's 'Human Practices' award, student teams have begun to incorporate biosecurity considerations into their research projects. For example, one student team at the 2010 iGEM Competition developed a software package called 'GenoTHREAT',[132] which is intended to help DNA synthesis companies detect possible sequences that could be used to produce Select Agents. In this instance, 'biosecurity thinking' is, quite literally, 'built-in' to the research experience, made an integral component of the research output.

These examples suggest that biosecurity awareness is growing within some segments of the 'synthetic biology community', and, in some instances, is becoming integral to the research experience. And, while a uniform definition of this new 'culture of responsibility' does not exist, the biosecurity messages outlined by Agent You, and other experts who have played a role in framing this new vision of responsibility, point to a change in research culture and practice. Codified in laboratory manuals and educational brochures; recorded on DVDs; presented at biosecurity workshops, these messages – including calls for "'enhanced watchfulness'" (PCSBI 2010, p. 145), for thinking about "the downsides of an experiment" (Amy Smithson), and for preventing the "exploitation or subversion" of scientific knowledge (Edward You) – describe a new orientation on risk management and an emerging set of responsibilities and moral obligations. Before concluding this chapter, I wish to reflect on the significance of this new orientation on risk management, one that favors a culture of 'prudent vigilance'.

While multiple biosecurity messages have been attached to recent calls for a new 'culture of responsibility', a common feature of these messages is that scientists should play a larger role in monitoring not only their own conduct, but also the conduct of those in their 'community'. In other words, scientists are encouraged not only to be prudent, but also vigilant. Whereas 'prudence' is a familiar aspect of life science culture and practice, exemplified by biosafety protocols that call for scientists to show discretion in the safe handling of biological materials, the concept of 'vigilance' is a relatively new addition to the lexicon of 'responsible life science'.

[132] See http://2010.igem.org/Team:VT-ENSIMAG/Genothreat.

This concept, I suggest, which signifies the emergence of biosecurity (rather than biosafety) as the primary site of regulatory concern in the US (Atlas 2005a), is bound up with a different way of thinking and talking about biological risks, and a new way of interacting with biology and biologists in (community) labs. For the synthetic biologists interviewed for my research, this is a significant development, even though they may not speak of their new responsibilities in terms of 'prudent vigilance'. Rather, they speak of 'biosecurity', of a research project's 'potential for deliberate misuse', and of 'getting to know their local WMD coordinator'.

As the DIYbio-FBI case suggests, it is with some ambivalence that (amateur) synthetic biologists engage in this new dialogue. While scientific fields such as nuclear physics have a relatively long tradition of engaging with security communities, and nuclear physicists have for some time been taught to consider the 'potential downsides' and 'security implications' of their work, this is not the case in the life sciences (observations that were touched on in the previous chapter in relation to the subject of censoring 'sensitive' scientific research). For DIY-biologists like Jason Bobe and Mackenzie Cowell, their engagement with the FBI is a new phenomenon, and they express a sense of uncertainty and unease about their new 'partnership' with law enforcement, and their new responsibilities as 'strategic partners' in biosecurity. As Bobe suggests, although it may be increasingly commonplace for DIY-biologists to know their 'local WMD Coordinator' (in Bobe's case, on a first-name basis), the presence of FBI field agents in DIYbio community labs is unfamiliar, and, for some, unsettling. Bobe also worries about the associations that have been made, if indirectly, between DIY-biology ('biohacking') and the theme of "weapons of mass destruction". He is concerned that some members of the DIYbio community may not wish to reach out to law enforcement for fear of exposing themselves to "legal liability", and even that some research activities may be "driven underground" (interview with Jason Bobe).

From the perspective of life scientists, it is, to some extent, unclear whether they are "suspects" or "saviors" (Atlas 2005a, p. 23) – 'allies' or 'potential threats' – and not just from outside their communities, but also from within. Biosecurity is said to demand 'enhanced watchfulness' on the part of the individual scientist, and

colleagues are to be monitored for 'suspicious behavior'. In the event that 'biosecurity risks' are identified, new lines of communication have been established to enable scientists to voice their suspicions to law enforcement agents. Agent You emphasized that it is important that synthetic biologists understand that "there is someone on your speed dial who you can contact and feel confident that you'll get the right response." Local WMD Coordinators are described as not only "the educators", but "also the bridge lines" (Edward You) – linking scientists with security experts – bridging not only a physical, but also a cultural divide (Relman 2010). At the same time, this biosecurity guidance is finite, as it is ultimately up to the individual scientist to negotiate 'real-world' scenarios, demonstrating their capacities as 'experts in biosecurity'. And while scientists may draw upon their lessons in biosecurity, and may request assistance from the FBI or other federal agencies at any time, the threshold of suspicion rests with the individual scientist, as only they (they are told) are "in a position to identify not only the risks and vulnerabilities, but also potential nefarious activity" (Edward You).

Yet, it aught to be underlined that the emerging 'partnership' between life science and security communities has not been imposed on scientists, nor have their responsibilities as 'strategic partners' in biosecurity. Recent connections between DIYbio and the FBI are not the result of coercion or the directed efforts of the FBI (or any one else) to expand the remit of security into new fields of science and technology. In other words, this is not a case of 'securitization', motivated by the overriding interests of security professionals or government elites (Wæver 1995). Rather, this engagement is voluntary – motivated by a sense of mutual benefit that has drawn science and security communities together in pursuit of a secure and sustainable 'scientific enterprise'. For Bobe, DIYbio's participation in biosecurity initiatives and their engagement with the FBI is viewed as helping maintain public support for their research activities, as well as offering their community the possibility of averting potentially more restrictive forms of oversight and regulation. More broadly, there exists a growing belief among life scientists that, in light of recent calls for censorship in life science publishing, 'self-governance' may very well provide the best means of protecting scientific freedom (Nature 2006).

For Agent You, and for others who endorse a 'self-policing' synthetic biology community (as one component of a wider regulatory regime), scientists are viewed as offering a promising and efficient means of defending against the threat of deliberate misuse. It is believed that by harnessing and directing the capacities of synthetic biologists to take on greater responsibility for biosecurity, they can both improve risk management efforts in the life sciences and enable a 'new generation' of scientists to be better prepared for a wider range of contingencies. Moreover, from a regulatory perspective, a greater reliance on 'self-governance' is viewed as reducing the 'costs' of regulation (Hutter 2005), allocating responsibility to those communities that are perceived to be the most knowledgeable about the risks engendered by their work. From this perspective, the FBI's biosecurity awareness raising efforts (and, in many ways, biosecurity awareness raising activities more broadly) can be understood as a practical attempt at enhancing 'national security' while minimizing more conventional ('top-down') regulatory demands.

In brief, for synthetic biologists and for security professionals, there exist legitimate reasons for wanting to raise biosecurity awareness. By some accounts, this approach to biosecurity is viewed as a common sense 'solution' to a seemingly intractable policy 'problem'. According to Piers Millett, a senior administrator for the BWC, a sensitized synthetic biology community – one capable of providing (at least in part) for its own biosecurity – is a "win-win." According to Millett, even if there is never a 'biosecurity incident', "[w]e end up with a generation of young, up-and-coming scientists who are aware of dual-use issues, and who appreciate the security implications of the biology they're doing." Yet, while one can hardly disagree with the sentiment that a 'risk-aware' 'synthetic biology community' offers appreciable benefits, in this section I have attempted to highlight that early signs of an emerging 'culture of responsibility' suggest that, for at least some (amateur) synthetic biologists, being an 'expert in biosecurity' – adopting a culture of 'prudent vigilance' – also carries potentially unforeseen consequences.

7.4 Conclusion

In this chapter, I have examined an approach to biosecurity that seeks to enable synthetic biologists to take on a greater role in ensuring the security and sustainability of their science. Unlike the biosecurity interventions discussed in the previous chapter, which are directed at controlling access to science, these interventions seek to encourage and enable synthetic biologists to (at least in part) 'govern themselves'. Although there is nothing novel about 'self-governance' as a mode of risk management in the life sciences – biosafety practices have relied on this principle for some time – what is unusual about the case of 'self-governance' in synthetic biology is that scientists are (more than ever before) encouraged to be, not only their own 'risk managers', but also their own 'police'. Visible in relation to new partnerships between science and security communities, and in relation to growing demands for 'prudent vigilance', this new vision of responsibility brings the worlds of science and national security into closer contact in the name of biosecurity, suggesting new opportunities, but also new challenges and dilemmas.

It is, I have argued, through a process of 'responsibilization' (Rose 2000) that this new orientation on risk management is presently being fostered, where the role of governmental actors and organizations engaged in aspects of biosecurity policy is to enable scientific communities to more effectively 'govern themselves'. Specifically, the aim of a number of biosecurity awareness raising activities directed at (amateur) synthetic biologists and discussed in this chapter is to enable a 'new generation' of scientists to become 'risk-aware', capable of actively contributing to biosecurity. In many ways, this process involves initiating scientists into "another world" (Edward You) – a world that is closely aligned with 'national security' considerations, and the traditional roles and responsibilities of law enforcement and security communities. On a conceptual level, this approach to risk management can be understood as a form of 'advanced liberal' government, exemplified by the notion of governing 'at a distance' (Rose 2000). Under this form of government, as Nikolas Rose suggests, "[i]ndividuals, families, firms, organizations, communities are urged

to take upon themselves the responsibility for the security of their property and their persons, and for that of their own families" (ibid, p. 327).

While enabling synthetic biologists to become their own 'experts in biosecurity' is viewed by many as a key element in a broader 'web of prevention' (which includes preventative controls on science, Chapter 6), holding out the possibility of enhanced security and a more sustainable science, there also exist doubts about this form of risk management. On the one hand, some believe synthetic biologists should not be permitted to 'self-regulate', as the risks are too great, and scientists may choose to act in their own self-interest. On the other hand, synthetic biologists are uncertain about the desirability of 'policing themselves'. As the DIYbio-FBI case suggests, scientists do not necessarily feel best suited to the task of biosecurity, nor do they necessarily wish to be held accountable for biosecurity risks. Scientists also express ambivalent attitudes about their engagement with law enforcement and security communities, and are concerned about the associations that have been made between (amateur) synthetic biology and 'weapons of mass destruction'. Indeed, one might argue that an unintended consequence of this new orientation on risk management – one that favors a culture of 'prudent vigilance' – is the introduction of a vocabulary and a way of thinking that serves to augment perceptions of synthetic biology and synthetic biologists, who are increasingly imagined as both 'biosecurity risks' and as 'strategic partners' in biosecurity.

8. Conclusion

8.1 Introduction

For the scientific and technical experts consulted for my research, there would appear to be little doubt that it is possible to 'identify', 'assess' and 'manage' synthetic biology's 'biosecurity risks'. Moreover, for these experts, preventing the deliberate misuse of synthetic biology and enabling its scientific and industrial potential are not mutually exclusive policy goals, but rather simultaneous objectives that constitute 'good governance'. Although there exist uncertainties about the nature of the risks themselves, and doubts about the suitability of familiar risk assessment techniques and the appropriateness of existing regulatory frameworks, there also exists an unyielding belief that it is possible to reconfigure even the most intractable 'uncertainties' as 'calculable risks' that can be managed. And, while the conviction to 'manage' risks that exist at the limits of scientific knowledge may, for some, suggest an attempt to "*feign control over the uncontrollable*" (Beck 2002, p. 41, emphasis in original), my thesis suggests this is not the case.

Contrary to the 'risk society' thesis (Beck 1992), my thesis demonstrates that, in the case of regulating synthetic biology, practical and legitimate efforts are being made to 'assess' and 'manage' risks that would appear to exceed the limits of scientific knowledge. Indeed, my thesis underlines that uncertainty is not an inhibition to risk management, but a call for more creative and more intensive methods of 'risk calculation' – an activity that is grounded in the belief that risks (once defined as 'risks' and not uncertain 'dangers') can be known with reasonable confidence and made the subject of regulatory intervention and control. Therefore, while the risk assessment techniques and risk management strategies that have been devised to govern synthetic biology may not 'fit' the technical ideal of risk, exemplified by 'quantitative risk assessment', they nonetheless aspire for 'reasoned estimation' and seek to inform and to justify responsible action in the face uncertainty. In this context, 'risk' can be conceptualized as an adaptive 'technique of

government', which is regularly adapted and deployed to achieve a variety of instrumental goals. In the absence of numbers, as I have shown throughout my thesis, other metrics – other ways of 'knowing' and 'intervening' – are brought to bear on complex policy 'problems' with a view to practical 'solutions'.

In this conclusion, I wish to reflect on how the 'risk regulation regime' (Hood et al. 2001) examined in my thesis is presently rendering (in practical and legitimate ways) synthetic biology 'governable', and how it is simultaneously producing a particular vision of an emerging science and its diverse practitioners that is not without consequence for our collective understanding of modern biology, its 'potential risks', and the kinds of 'responsibility' deemed necessary to manage these risks. In doing so, I will highlight several key themes that have emerged through the course of my research, which, on the one hand, underline risk's capacity as an adaptive 'technique of government', and, on the other, its capacity to both describe and produce the very 'risks' it seeks to visualize and control. The risk management process discussed here, and throughout my thesis, is one that enables new space for thought and action, while simultaneously limiting the scope of what can be expected of synthetic biology. Not only contributing to the advancement of risk theory in sociology that challenges the 'risk society' thesis (Beck 1992), on the grounds that complex technological hazards are *currently* being governed through an assortment of "technical means for intervening in reality for the achievement of specific ends" (Dean 1999, p. 184), this research also sheds light on the performative dimensions of a regulatory process that envisions advances in modern biology as posing a 'bioterrorist threat', requiring some sort of 'biosecurity response'.

8.2 Risk calculation in the absence of numbers

The claim that we are living in a 'post-risk calculation' world (Beck 2009) does not account for the regulatory response that has been mounted to address the perceived biosecurity risks posed by synthetic biology. The technical challenges associated with calculating risk estimates linked with arbitrary sequence information submitted to DNA synthesis providers, as well as the uncertainties that surround the

unknown identities and motives of prospective customers, has not prevented the Department of Health and Human Services (DHHS 2010b) from introducing regulatory guidelines that seek to establish a more or less structured risk management procedure for industry to follow. The very fact that industry has produced its own (more rigorous) guidelines and that orders for 'synthetic double-stranded DNA' are presently being processed by companies that have little to no 'appetite for risk' is a testament to an industry that has not abandoned the belief that risks can be known with reasonable confidence, and that these risks can be managed. If it were otherwise – if limitless precaution in the face of extreme uncertainty had suddenly emerged – industry would shut its doors.

This observation is not limited to the case of the DNA synthesis industry, but rather it extends to all aspects of the ongoing regulatory response in synthetic biology, whether one considers the case of 'dual-use research' or 'do-it-yourself (DIY) biology'. Although there exist worries about publishing scientific protocols that could provide a 'blueprint for bioterrorism' and fears about 'biohackers' building novel pathogens in their garage, concerted efforts are being made to manage these risks, with the effect of enabling synthetic biology to move forward. Specifically, new policy on 'dual-use research of concern' (DHHS 2012) has been devised to anticipate and prevent access to 'dangerous knowledge', and the Federal Bureau of Investigation's (FBI) outreach and awareness raising activities have begun to educate 'non-institutional biologists' on how to 'police themselves'. Furthermore, and perhaps of greatest interest to risk theorists who ascribe to Ulrich Beck's (1992) 'risk society' thesis, this will-to-order uncertainty and to establish regulatory controls has occurred despite doubts about how to calculate risks for which little can be known on the basis of statistical calculation.

To date, there has never been a bioterrorist attack involving synthetic biology, and thus statistical data on the 'likelihood' and 'consequences' – the standard metrics that define the traditional risk assessment model – of a possible future attack do not exist. There are no numbers to be added to spreadsheets, no probabilities to be calculated, and thus statistics cannot offer a window onto the future of synthetic biology's possible risks. Yet, the fact remains, in the context of

synthetic biology, as in other domains of 'science policy' characterized by "intrinsic, irreducible uncertainty" (Majone 2010, p. 99), risk assessments are being conducted and risk management decisions are being made. In the absence of "meaningful statistics", risk assessment does not reach its limit, but rather a variety of other 'ways of knowing' are brought to bear on an uncertain future, which are used to inform and to justify risk management decisions (Erickson and Doyle 2004, p. 18). In this light, what should be the focus of critical attention is not the absence of statistics, but rather the presence of a variety of alternative risk-based techniques that are deployed beyond the frontier of statistical calculation (O'Malley 2004). If for no other reason, one might argue, than because these alternatives exist, and they can tell us a great deal about the manner in which problematic people and things are constituted as 'risks' to be managed, and what is at stake in doing so. In the case of synthetic biology, to suggest otherwise would be to overlook much of the regulatory process itself and the many risk-based judgments and justifications that are used to enable action in the present, beyond 'quantitative risk calculation'.

Throughout my thesis, I have explored a variety of calculative techniques and regulatory strategies that are used to organize uncertainty and enable choice and decision (Power 2007), few of which can be said to satisfy the stringent conditions of 'quantitative risk assessment'. In the case of genetic engineering, for example, a regulatory framework (Office of Science Technology and Policy 1986) was designed to anticipate and control potentially 'novel' risks that regulators sought to 'calculate' not on the basis of probability estimates and loss figures associated with recombinant organisms, but on the basis of inference to the 'natural templates' from which these organisms might be derived. Today, synthetic biology, having introduced the possibility of 'non-natural templates', or 'DNA sequences that do not exist in nature', is believed to have removed even this foothold on scientific knowledge, introducing new uncertainties and new problems of measurement. As one senior biodefense scientist expressed about synthetic sequences, introduced in Chapter 5, "without a [natural] template, where's the risk?" Under these circumstances, if regulators relied only on 'quantitative risk assessment', there would be an immovable obstacle between 'risk identification' and 'risk

management', as the 'risks' in question could not be 'calculated', and unlimited precaution, one might imagine, could be the order of the day.

But, this is not the case in synthetic biology, just as it was not the case in genetic engineering, and not because 'quantitative risk assessment' is not valued (in fact, it remains a regulatory ideal), but because 'risk' is everywhere. As François Ewald (1991, p. 199) reminds us: "Nothing is a risk in itself; there is no risk in reality", yet "anything *can* be a risk", because risk "is first and foremost a schema of rationality, a way of breaking down, rearranging, ordering certain elements of reality". Risk, in brief, is a category of understanding, a way of analyzing potential events in such a way that they might be governed. In this light, one might argue, if risk assessment does indeed have a 'limit', this limit is constrained by human ingenuity to 'break down' and 'rearrange' diverse 'elements of reality', enabling them to be made objects of thought and action, not by a lack of probabilistic knowledge about the world. Therefore, the question, "without a [natural] template, where's the risk?", although drawing attention to an important source of uncertainty, does in fact have an answer, indeed it has multiple answers. This is because the question might equally be posed, 'how does one re-imagine non-natural templates, so they can be understood as risks?' And, it is the latter question, not the former, that is most characteristic of the thinking and practical work of scientific and technical experts seeking 'solutions' to the 'problem' of synthetic biology.

In the absence of scientific evidence – in the absence of numbers – other forms of knowledge and modes of calculation are used to 'break down' and 'rearrange' the diverse elements that makeup 'synthetic biology' and its 'potential risks'. As the case of the National Institutes of Health's (NIH 2011) guidelines on research involving recombinant DNA molecules can attest (introduced in Chapter 5), although barriers to 'knowing the risks' are regularly identified, they are also overcome. In this instance, the very definition of 'recombinant DNA molecules' was redefined to include those comprised of 'synthetic sequences', or 'DNA that does not exist in nature', enabling synthetically derived molecules and synthetically derived organisms to be treated 'as if' they are natural for the purposes of oversight and regulation. And, while this is (or was) only one source of scientific uncertainty in

synthetic biology, it underlines that 'uncertainty' is not viewed as an insurmountable obstacle to risk assessment and risk management, but rather as a call to action, (re)invention and adaptation in the face of uncertainty.

In the case of the synthetic biology regulatory process, 'ingenuity' is not lacking. On the contrary, it is integral to the design and implementation of biosecurity interventions that seek to 'secure' and 'sustain' an emerging science that does not lend itself to 'quantitative risk assessment'. And, while numbers and statistical methods rarely feature in the risk assessments discussed in this thesis, experts nonetheless appeal to a scientific rationality; they aspire to technical mastery of science over chance, and seek to satisfy highly instrumental aims. Just because 'quantitative risk calculation' is absent, does not mean that 'calculation' itself is absent, merely that it takes other forms. Indeed, as governmentality theorists contend (Dean 1999; Rose 2002; O'Malley 2004), there is no 'singular' or 'best' way to govern an indeterminate future, no monolithic 'risk technology' or 'risk rationality', which, once exceeded, relegates individuals, families, communities, organizations or nations to a state of epistemological stasis, indifference or inaction. There is, in fact, if one takes seriously existing sites of risk assessment such as the one examined in this thesis, 'no risk beyond risk'. The case of regulating synthetic biology, underscores that 'risk' and 'risk thinking' do indeed take on multiple and heterogeneous configurations, are infinitely adaptable, and directed at achieving practical outcomes that are, above all, believed to be *possible* (ibid.).

8.3 Managing risk management processes

In the absence of numbers, other modes of calculation are invented, which are no less based on a scientific rationality that conceives of 'risks' as objective facts that can be understood and brought under frameworks of technical intervention and control. Of particular significance in relation to governing synthetic biology is the design and construction of risk management processes, procedures and protocols that can be used to guide and to justify practical action in the face uncertainty. Manifest in federal guidance on how to screen potentially dangerous 'sequences'

and 'customers' (DHHS 2010b), 'checklists' that are used to identify 'dual-use research of concern' (NSABB 2007), and 'table top exercises' that seek to enable synthetic biologists to become their own 'experts in biosecurity', risk management in synthetic biology depends upon, and is indeed defined by, its capacity to produce prescriptive guidance that 'breaks down', 'rearranges' and provides 'recipes' to prevent the deliberate misuse of biotechnology. It is in the form of these visionary documents and blueprints that the highly uncertain world of synthetic biology and bioterrorism are rendered knowable and actionable. It is by way of deconstructing the 'synthetic biology threat' and refashioning its constituent parts through language, embodied in new categories and concepts, that risk assessors and risk managers (representing federal agencies, DNA synthesis companies, scientific committees, and so on) lay bare the complexities of bioterrorism and make it possible – through a 'hybrid' activity known as 'regulatory science' – to both assess and manage unwieldy, seemingly unknowable, contingencies.

On the one hand, documents such the *Screening Framework* (DHHS 2010b), which break down biosecurity risk assessment into 'sequence screening' and 'customer screening', can be understood as sites of creation and innovation, in as much as ideas such as 'controlled sequences' and 'restricted persons' (and the many sub-components and descriptors that go along with them) ascribe a form of materiality to particular kinds of people and things to be governed. On the other hand, documents of this kind are the manifestation of regulatory strategizing, conceived by scientific and technical experts assigned a highly instrumental task, namely, to prevent 'dangerous tools' from reaching 'dangerous hands', offering the essential methodologies and frameworks for biosecurity 'best practices'. They are programmatic, ideational, and didactic, designed to teach their target audience ('screeners', (amateur) biologists, institutional biosafety committees) how to assess risks effectively, and how to become their own risk managers.

In this light, much of the work of governmental actors and organizations, I have argued, is not so much to assess and manage synthetic biology's biosecurity risks, but to manage the risk management process itself, to enable risk managers or "processors of uncertainty" (Power 2007, p. 9) to be responsible for the day-to-day

oversight and operations of companies, institutions, and (non-institutional) lab spaces. This distinctly modern form of governing has been described as 'advanced liberal' (Rose 2000) and is characteristic of much of the practical work of administering people and things in the twenty-first century. Michael Power has described this approach to risk management as the "new governmentality" (Power 2007, p. 41), one that prizes "the organization of uncertainty in the form of frameworks which emphasize management *process* in a field hitherto dominated by experts in risk *analysis*" (ibid, p. 36). It is in this new regulatory, increasingly 'managerial', environment that the organization of uncertainty is mobilized, not so much with a view to technical precision and numeric supremacy, but with a view to the coherency and procedural clarity of technical frameworks and written guidance. In this context, as I argued in Chapter 6, the strengths of policy proposals are valued not only for their scientific rigor, but also for their administrative merits. In many ways, as Power rightly argues: "A cultural 'trust in numbers' has given way to an emphasis on systems and processes to define governance" (ibid, p. 178).

8.4 Pragmatic policymaking

In practice, I have argued, the regulatory process in synthetic biology is characterized by 'pragmatic policymaking', a flexible approach to policy design premised upon the belief that biosecurity risks can be assessed, rendered knowable, and made the subject of regulatory interventions that can be used to satisfy a variety policy objectives, including, but not limited to, mitigating the 'likelihood' and 'consequences' of possible future harm. Indeed, mitigating risk (the physical sort), although unquestionably a significant source of concern for scientists, security experts, and science policymakers (among others), is only one preoccupation that motivates the design of 'optimal' science policies. In the case of synthetic biology, as in the case of genetic engineering, there is an apparent conviction that it is not enough to prevent risks, but to prevent them in such a way that the science is protected, that its industrial potential is fulfilled, and that the risks in question do not exceed the technical or administrative capacities of regulation itself.

This pragmatic belief and apparent conviction can be seen in all elements of the regulatory response to the problem of deliberate misuse in synthetic biology. As I have argued throughout my thesis, it is visible in the form of recurrent concerns about 'novel' risks, risks that are: 'beyond assessment'; that do not 'match-up' with existing regulatory frameworks; that are too uncertain to be conceived as 'risks' at all. Yet, in each case, these voiced concerns and uncertainties are overcome: anticipated 'dangers' (for example, arbitrary sequence information) are re-imagined as 'potential risks' (for example, sequence information describing Select Agents, 'sequences of concern') or simply passed over on account of the 'limits of prediction' (for example, sequence information corresponding with pathogens that do not exist in nature); potential risks are made to 'fit' existing regulatory frameworks (for example, the Select Agent Regulations); guidelines are amended to enable 'synthetic DNA' to be treated as if it is 'natural DNA' (NIH 2011), and new 'biosecurity' provisions are grafted on to existing 'biosafety' protocols (CDC/NIH 2009). In this manner, pragmatic policymaking can be seen to favor efficiency; it does not yield to scientific uncertainty, and is, above all, ends-driven.

Evidence of 'pragmatic policymaking' is equally visible in the efforts of diverse governmental actors and organizations that seek to enable a 'secure' and 'sustainable' science. Here, pragmatism permeates a regulatory discourse that self-consciously reflects on the need to balance potentially competing policy objectives: weighing demands for 'national security' against 'scientific freedom', 'industrial productivity' against 'prudential oversight'; averting blame for doing 'too little to regulate' or for doing 'too much'; alleviating fears about 'bioterrorism' while nurturing hopes for 'bioeconomy'. These are among the many faces of risk management and regulation that characterize the regulatory process examined in this thesis, and which help shape the design and production of risk management strategies, as well as their visible 'traces' (guidelines, checklists, articles, and so on). In brief, there is a need, or at least a perceived need, to balance (and be seen to balance) sharply contrasting expectations and competing political imperatives, minimizing not only the 'primary risks' associated with 'deliberate misuse' but also the 'secondary risks' associated with the reputations of those engaged in various

aspects of the synthetic biology regulatory response. In this regard, it should be recalled that the very notion of 'risk' plays a functional role in enabling and justifying regulatory decisions. As Rothstein et al. observe:

> "Constructing regulatory problems as risk problems offers a solution to regulators by providing a procedural rationality for managing societal risks in ways that meet bureaucratic and legal demands for processes that are rationally consistent, organized and defensible." (2006, pp. 100-101)

While 'pragmatism' of this kind might be dismissed by some as evidence of concealed interests or a lack of honesty on the part of various regulators who cannot control the risks they claim to understand, a view that would align with aspects of the 'risk society' thesis, there is an alternative interpretation, one that aligns much more closely with the case of synthetic biology. As Mitchell Dean (1999) has argued, regimes of government are characterized by a distinctly 'utopian element' that cannot be dissociated from governmental processes and mentalities of government. To paraphrase Dean (ibid, p. 33), 'every theory or programme of government presupposes a better world, and thus is not only concerned about administrating people and things, but also about leading them to a better existence'. In the case of synthetic biology, understanding that this 'utopian element' exists, and that it is in fact intrinsic to how regimes of government and administration operate (ibid.), can help clarify what might otherwise be dismissed as evidence for a regulatory process that was decided before it began, which is not the case. What is the case is that 'governing through risk' is about much more than simply eliminating uncertainty about possible future harm. It is about shaping the present in such a way that future objectives and aspirations may (in time) be realized.

8.5 Bio(in)security

There exists one further theme that is equally apparent in my thesis, and this can be traced to the very language, concepts, categories, and behaviors that characterize biosecurity in synthetic biology, and contemporary biosecurity practices more broadly. Specifically, the case of synthetic biology underlines that the worlds of

'national security' and the 'life sciences' are increasingly intertwined, and not without consequence for how biologists, science policymakers, security experts, journal editors (indeed, all of us) understand, represent and interact with modern biology. Today, more than ever before, advances in biotechnology are accompanied by an expectation of 'deliberate misuse' and 'catastrophic harm', and are bound up with a new set of vocabularies describing 'controlled sequences', 'malicious parts', 'dual-use research of concern', 'denied persons' and 'prudent vigilance', concepts that suggest a new orientation on life science research, its 'potential risks', and the forms of 'risk responsibility' needed to manage these risks.

For the scientific and technical experts consulted for my research, this new way of interacting with, and talking about, biotechnology is increasingly self-evident. In the case of the *Screening Framework* (DHHS 2010b), it is assumed that 'sequences of concern' are a natural extension of the 'Select Agent List'; multiple lists of 'denied persons' are described as an 'administrative challenge' ('they should all be in one place'), but lists of this sort are assumed to be necessary and of obvious value to DNA synthesis providers. For life science publishers, biosecurity oversight committees, and the World Health Organization, the concept of 'dual-use research of concern' has (very recently) taken on a distinct meaning; it is recognized as a 'potential risk'; watched out for; deliberated on, and possibly (if not now, then "in the very near future") it will need to be restricted to those "who have a legitimate need to know" (NSABB 2012, p. 6). For DIY-biologists, it is believed to be essential to demonstrate their 'biosecurity awareness', to engage with the FBI, and to guard against 'potential transgressions' within their 'community'.

It is with a view to these new interactions and emerging vocabularies that one can see that the perceived threat of bioterrorism is not only reconfiguring the defensive architectures used to control biology – from 'biosafety' to 'biosecurity'; from controlling 'dangerous pathogens' to controlling 'dangerous knowledge'; from 'self-governance' to 'self-policing' – but also our collective expectations for modern biology. In the US context, it is all but taken-for-granted that to speak of 'biosecurity' in relation to synthetic biology is common sense – a logical response to the fact that the science could 'democratize' bioengineering, enabling more people in more

places to participate in modern biology. In government working groups and biotech company boardrooms, it is apparent that DNA synthesis technology poses 'biosecurity risks', and that innovative 'biosecurity solutions' are needed. For DIY-biologists, it is increasingly commonplace to 'know their local WMD coordinator' and to engage with law enforcement and security communities.

There are, of course, many more concepts, categories, and interactions of this kind that I could revisit, but what I wish to highlight here is merely that these concepts, categories and interactions are relatively new, and are increasingly taken-for-granted. For many, biosecurity, and its associated vocabularies and rituals, has taken on a highly specific meaning and a distinct functionality – on the one hand, enabling the communication of biosecurity 'best practices' and, on the other, enabling these practices to be made routine. As Ian Hacking (1992) reminds us, the naming and classification of new 'risks' is not simply an administrative or calculative activity that describes the world 'out there', but it is also performative, bringing new kinds of people and things into being hand-in-hand with their naming (ibid.). Thus, to speak of synthetic biology's 'biosecurity risks' carries an ontological significance beyond epistemological debates on risk as a 'mode of measurement'. Indeed, the very act of naming new biosecurity risks transfers material and political significance to formally unspeakable worries and dilemmas.

8.6 Governing through risk

Finally, given the centrality of 'risk regulatory concepts' (Fisher 2010), such as 'risk', 'risk assessment' and 'risk management', to contemporary regulatory discourses, one might ask: To what extent is 'risk' (and not just the language of risk) actually deployed in the case of regulating synthetic biology? To what extent is synthetic biology actually 'governed through risk'? Throughout my thesis, I have, indeed, noted that the language of risk, especially appeals to the notion of 'quantitative risk assessment' (and its components, the vocabulary of 'likelihood' and 'consequences'), is commonly deployed in a manner that is inconsistent with the 'technical ideal' of risk, traditionally conceived as an 'objective' mode of measurement and decision-

making. In other words, the language of risk can clearly be seen to play a rhetorical function. Yet, as I have also underlined throughout my thesis, this technical ideal does not capture the range of risk assessment techniques that are, in practice, regularly used to 'calculate' the seemingly 'incalculable'. Nor should this observation be surprising, as the technical ideal of 'objective' risk assessment and 'value-neutral' policymaking is, and always was, unachievable in practice. This is because the future cannot be known with certainty, and thus decisions, no matter how 'rigorous' the assessment, must be made on the basis of imperfect knowledge.

In this thesis, I have examined a range of calculative techniques and regulatory strategies that are, in a highly instrumental sense, enabling synthetic biology to be governed. And, while these techniques and strategies scarcely resemble the technical ideal of 'quantitative risk assessment', they serve a very similar function. That is, they attempt to impose order on the world, appealing to a scientific rationality that assumes that risks can be known with reasonable confidence and be made the subject of technical intervention and control. Indeed, it is this scientific rationality that unites diverse experts – ranging from public health officials to biological weapons experts – in their individual and collective efforts to 'assess' and 'manage' risks that would appear, at times, to not be 'risks' at all, but rather incalculable 'dangers', for which one does not have, and cannot have, the "knowledge or the measure" (Ewald 2002, p. 294). If their efforts can tell us anything, it is that even beyond the remit of scientific knowledge and the limits of statistical prediction, there exists the capacity – and the will – to order uncertainty in the face of an unknown future, enabling action in the present.

Of course, acknowledging the versatility of risk, as an adaptive 'technique of government', permits much more than a general recognition of alternative modes of risk calculation. That is, it permits an analysis of diverse sites of risk assessment and risk management that are not only testing the limits of human ingenuity to organize uncertainty, but also (re)fashioning reality in highly specific ways. Risk calculation both produces order where there is disorder and reifies anxieties about possible future harms that may never happen, but, once conceived as 'risks', must be taken seriously; made the subject of deliberation, monitoring and management. Thus, the

claim that we are living a in a 'post-risk calculation' world does not just narrow the scope of what should count as legitimate risk assessment, but also threatens to limit our sense of intrigue about risk management activities that are having a very real impact on contemporary life. Thus, such a perspective is not only analytically constraining, but also ethically problematic, because it fails to take seriously the pragmatic efforts of diverse social actors and organizations that are presently governing through risk, and shaping the world around us.

Appendix A: List of interviewees

1. **Volker Beck** – Senior biodefense scientist and biological weapons expert – Advisor to the German Foreign Office (now a freelance CBRN expert)
2. **Jason Bobe** – DIY-biologist – Co-founder of DIYbio; Executive Director of PersonalGenomes.org and Director of Community for the Personal Genome Project based out of George Church's lab at Harvard Medical School
3. **Rob Carlson** – Synthetic biologist – Principal at Biodesic, an engineering and strategic consulting firm in Seattle that provides services to governments and corporations around the globe
4. **Mackenzie Cowell** – DIY-biologist – Co-founder of DIYbio
5. **Malcolm Dando** – Biological weapons expert – Professor of International Security at the University of Bradford, and co-director of its project on strengthening the Biological and Toxin Weapons Convention
6. **Drew Endy** – Synthetic biologist – Assistant Professor, Department of Bioengineering, Stanford University
7. **David Franz** – Senior biodefense scientist and biological weapons expert – Former head of USAMRIID; Committee Member on the Fink Committee
8. **Marius Grinius** – Arms control and disarmament expert – Canadian Ambassador and Permanent Representative to the Office of the United Nations and to the United Nations Conference on Disarmament (now retired)
9. **Andrew Hessel** – Synthetic biologist and futurist – Distinguished Researcher with Autodesk Inc.'s Bio/Nano Programmable Matter group, based out of San Francisco; co-founder of the Pink Army Cooperative, the world's first cooperative biotechnology company
10. **Iris Hunger** – Biological weapons expert – Head of the Hamburg Research Group for Biological Arms Control (now with the Federal Information Centre for Biological Security at the Robert Koch Institute in Berlin)

11. **Stephen M. Maurer** – Lawyer, educator and author – Adjunct Associate Professor and Director of the Goldman School Project on Information Technology and Homeland Security, University of California Berkley
12. **Piers Millett** – Biological weapons expert – Political Affairs Officer for the Implementation Support Unit of the Biological Weapons Convention
13. **Christopher Park** – Counter-bioterrorism specialist – Senior Advisor for Bioterrorism in the Bureau of International Security and Nonproliferation at the US Department of State (now Director of the Biological Policy Staff); contributor to the development of the *Screening Framework*
14. **Dana Perkins** – Public health official and biological weapons expert – Public health official working for the US DHHS (now working for the United Nations Security Council 1540 Committee); contributor to the development of the *Screening Framework*
15. **Amy Smithson** – Chemical and biological weapons expert – Senior Fellow at the James Martin Center for Nonproliferation Studies, Washington DC Office
16. **Edward You** – Counter-bioterrorism law enforcement agent – Supervisory Special Agent in the FBI's Weapons of Mass Destruction Directorate, Biological Countermeasures Unit
17. **Richard Weller** – Senior biodefense scientist and biological weapons expert – Senior Program Manager in the Biological Sciences Division at the Pacific Northwest National Laboratory
18. **Anonymous** – Senior biodefense scientist and biological weapons expert, United Kingdom
19. **Anonymous** – Senior biodefense scientist and biological weapons expert, Australia
20. **Anonymous** – Senior biodefense scientist and biological weapons expert, United Nations Office for Disarmament Affairs

References

Aradau, C. and van Munster, R. (2007). Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13(1): 89–115.

Aradau, C. and van Munster, R. (2008). Taming the future: the dispositif of risk in the war on terror. In: L. Amoore and M. de Goede (eds.) *Risk and the War on Terror*. London: Routledge.

Aronson, N. (1982). Nutrition as a social problem: A case study of entrepreneurial strategy in science. *Social Problems* 29(5): 474-487.

Atkinson, P. and Hammersley, M. (1994). Ethnography and participant observation. In: N.K. Denzin and Y.S. Lincoln (eds.) *Handbook of qualitative research*. Thousand Oaks: Sage Publications Ltd.

Atlas, R.M. (2003). Science publishing in the age of bioterrorism. *Academe* 89(5): 14–18.

Atlas, R.M. (2005a). Biosecurity concerns: Changing the face of academic research. *Chemical Health and Safety* 12(3): 15-23.

Atlas, R.M. (2005b). Ensuring Biosecurity and Biosafety through Biopolicy Mechanisms: Addressing Threats of Bioterrorism and Biowarfare. *Asian Biotechnology and Development Review* 8(1): 121-137.

Atlas, R.M. and Dando, M. (2006). The Dual-Use Dilemma for the Life Sciences: Perspectives, Conundrums, and Global Solutions. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 4(3): 276-286.

Atlas, R.M. (2009). Responsible Conduct by Life Scientists in an Age of Terrorism. *Science and Engineering Ethics* 15(3): 293-301.

Austin, J.L. (1955). *How to do Things with Words: The William James Lectures delivered at Harvard University in 1955*. J. O. Urmson and Marina Sbisà (eds.). Oxford: Clarendon.

Ayres, I. and Braithwaite, J. (1991). Tripartism: Regulatory capture and empowerment. *Law and Social Inquiry* 16(3): 435-496.

Ball, P. (2004). Starting from scratch. *Nature* 431(7009): 624-626.

Balmer, A. and Martin, P. (2008). *Synthetic biology: Social and ethical challenges*. An independent review commissioned by the Biotechnology and Biological Sciences Research Council (BBSRC), available at: http://www.bbsrc.ac.uk/documents/0806-synthetic-biology-pdf/.

Beck, U. (1992). *The Risk Society: Towards a New Modernity*. London: Sage.

Beck, U. (2002). The Terrorist Threat: World Risk Society Revisited. *Theory, Culture & Society* 19(4): 39–55.

Beck, U. (2009). *World at Risk*. Cambridge: Polity Press.

Belson, N.A. (2000). US regulation of agricultural biotechnology: An overview. *AgBioForum* 3(4): 268-280.

Benner, S.A. and Sismour, A.M. (2005). Synthetic biology. *Nature Reviews Genetics* 6 (July): 533–543.

Bennett, G., Gilman, N., Stavrianakis, A., and Rabinow, P. (2009). From synthetic biology to biohacking: are we prepared? *Nature Biotechnology* 27(12): 1109-1111.

Berger, P.L. and Luckmann, T. (1966). *The social construction of reality: A treatise in the sociology of knowledge*. London: Penguin Books.

Berger, K.B., Pinard, W., Coat, G. and Epstein G.L. (2010). *Minimizing the Risks of Synthetic DNA: Scientists' views on the U.S. Government's Guidance on Synthetic Genomics*, summary of 11 January 2010 meeting, prepared by AAAS Center for Science, Technology and Security Policy, available at: http://cstsp.aaas.org/files/syn%20bio%20summary%20012110.pdf.

Bernauer, H. et al. (2008). *Technical solutions for biosecurity in synthetic biology*. Report on the "Workshop Technical solutions for biosecurity in synthetic biology", organized by the Industry Association Synthetic Biology (IASB), 3 April 2008, Munich, available at: http://www.synbiosafe.eu/uploads///pdf/iasb_report_biosecurity_syntheticbiology.pdf.

Berns et al. (2012). Policy: Adaptations of avian flu virus are a cause for concern. *Nature* 482(7384): 153-154.

Bigo, D. (2000). When two become one: Internal and external securitisations in Europe. In: M. Kelstrup and M.C. Williams (eds.) *International relations theory and the politics of European integration: Power, security and community*. London: Routledge.

Bigo, D. (2006). Globalized-In-Security: The Field and the Ban-opticon. In: J. Solomon and N. Sakai (eds.) *Translation, Biopolitics and Colonial Difference*. Hong Kong: Hong Kong University Press.

Black, J. (2010). Risk-based regulation: Choices, practices and lessons being learnt. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Blok, A., Jensen, M. and Kaltoft, P. (2008). Social identities and risk: Expert and lay imaginations on pesticide use. *Public Understanding of Science* 17(2): 189-209.

Blumer, H. (1971). Social problems as collective behavior. *Social Problems* 18(3): 298-306.

Boswell, C. (2014). *The political uses of expert knowledge: Immigration policy and social research*. Cambridge: Cambridge University Press.

Bounds (2010). Challenges to designing regulatory policy frameworks to manage risks. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Bradbury, J.A. (1989). The Policy Implications of Differing Concepts of Risk. *Science, Technology & Human Values* 14(4): 380-399.

Braithwaite, J. (1982). Enforced self-regulation: A new strategy for corporate crime control. *Michigan Law Review* 80(7): 1466-1507.

Bügl et al. (2007). DNA synthesis and biological security. *Nature Biotechnology* 25(6): 627-629.

Bunton, R. and Peterson, A. (eds.) (2005). *Genetic governance: Health, risk and ethics in the biotech era*. Milton Park: Routledge.

Burchell, G., Gordon, C. and Miller, P. (eds.) (1991). *Foucault effect: Studies in governmentality*. Chicago: University of Chicago Press.

Butler, J. (1993). *Bodies That Matter: On the Discursive Limits of "Sex"*. New York: Random House.

Caduff, C. (2008). Anticipations of Biosecurity. In: A. Lakoff and S.J. Collier (eds.) *Biosecurity Interventions: Global Health and Security in Question*. New York: Columbia University Press.

Carlson, R. (2008). Tracking the spread of biological technologies. *Bulletin of Atomic Scientists*, 21 November 2008, available at: http://thebulletin.org/tracking-spread-biological-technologies.

Carlson, R. (2009). The Changing Economics of DNA Synthesis. *Nature Biotechnology* 27: 1091-1094.

Castel, R. (1991). From dangerousness to risk. In: G. Burchell, C. Gordon and P. Miller (eds.) *Foucault effect: Studies in governmentality*. Chicago: University of Chicago Press.

Campbell, P. (2006). Empowerment and restraint in scientific communication. *EMBO reports* 7: S18-S22.

Casadevall, A. and Pirofski, L. (2004). The weapon potential of a microbe. *TRENDS in Microbiology* 12(6): 259-263.

Casadevall, A. and Shenk, T. (2012). The H5N1 Moratorium Controversy and Debate. *mBio* 3(5): 1-2.

CASE Collective (2006). Critical Approaches to Security in Europe: A Networked Manifesto. *Security Dialogue* 37(4): 443–87.

Cello, J., Paul, A.V. and Wimmer, E. (2002). Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template. *Science* 297(5583): 1016–1018.

Centers for Disease Control and Prevention and the National Institutes of Health (1999). *Biosafety in Microbiological and Biomedical Laboratories* 4th Edition, available in print.

Centers for Disease Control and Prevention and the National Institutes of Health (2009). *Biosafety in Microbiological and Biomedical Laboratories* 5th Edition, available at: http://www.cdc.gov/biosafety/publications/bmbl5/BMBL.pdf.

Check, E. (2003). US officials urge biologists to vet publications for bioterror risk. *Nature* 421: 197.

Check, E. (2005). Synthetic biologists face up to security issues. *Nature* 436: 894-895.

Check, E. (2009). Keeping genes out of terrorists' hands. *Nature* 461(7260): 22.

Church, G. (2005). Let us go forth and safely multiply. *Nature* 438: 423.

Chyba, C.F. and Greninger, A.L. (2004) Biotechnology and Bioterrorism: An Unprecedented World. *Survival* 46(2): 143-162.

Chyba, C.F. (2006). Biotechnology and the Challenge to Arms Control. *Arms Control Today* 36(8): 11-17.

Coglianese, C. (2010). Management-based regulation: Implications for public policy. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Collier, S.J., Lakoff, A. and Rabinow, P. (2004). Biosecurity: Towards an anthropology of the contemporary. *Anthropology Today* 20(5): 3-7.

Collier, S.J. and Lakoff, A. (eds.) (2008). *Biosecurity Interventions: Global Health and Security in Question*. New York: Columbia University Press.

Cooper, M. (2006). Pre-empting Emergence: The Biological Turn in the War on Terror. *Theory, Culture & Society* 23(4): 113–135.

Corbridge, S., Williams, G., Srivastava, M. and Véron, R. (2005). *Seeing the state: Governance and governmentality in India*. Cambridge: Cambridge University Press.

Coyle, A. (2007). Discourse analysis. In: E. Lyons and A. Coyle (eds.) *Analysing qualitative data in psychology*. London: Sage Publications Ltd.

Cunningham-Burely, S. and Kerr, A. (1999). Defining the 'social'. *Sociology of Health & Illness* 21(5): 647–668.

Davis Cross, M.K. (2013). Rethinking epistemic communities twenty years later. *Review of International Studies* 39(1): 137-160.

Dean, M. (1999). *Governmentality: Power and rule in modern society*. London: Sage Publications Ltd.

Defense Science Board (1997). *The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats*, Vol. I, Final Report, October 1997. Washington DC, available at: http://www.theblackvault.com/documents/trans.pdf.

Denzin, N.K. (2004). Symbolic interactionism. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Department of Health and Human Services (2009*). Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA* (first draft), available at: http://www.gpo.gov/fdsys/pkg/FR-2009-11-27/html/E9-28328.htm.

Department of Health and Human Services (2010a). *Response to Public Comments on draft Screening Framework Guidance for Synthetic Double-Stranded DNA Providers*, available at:

http://www.phe.gov/Preparedness/legal/guidance/syndna/Documents/syndna-commentsresponse.pdf.

Department of Health and Human Services (2010b). *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA* (final version), available at: http://www.phe.gov/Preparedness/legal/guidance/syndna/Documents/syndna-guidance.pdf.

Department of Health and Human Services (2010c). 'Frequently Asked Questions: Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA', available at: http://www.phe.gov/Preparedness/legal/guidance/syndna/Pages/faqs.aspx.

Department of Health and Human Services (2012). *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern*, available at: http://oba.od.nih.gov/oba/biosecurity/pdf/united_states_government_policy_for_oversight_of_durc_final_version_032812.pdf.

Deplazes, A. (2009). Piecing together a puzzle: An exposition of synthetic biology. *EMBO reports* 10(5): 428-432.

De Vriend, H. (2006). *Constructing Life: Early social reflections on the emerging field of synthetic biology*. The Hague: Rathenau Institute; Working Document 97.

Douglas , T. and Savulescu, J. (2010). Synthetic biology and the ethics of knowledge. *Journal of Medical Ethics* 36: 687-693.

Endy, D. (2005). Foundations for engineering biology. *Nature* 438(24): 449–453.

Enserink, M. and Malakoff, D. (2012). Will flu papers lead to new research oversight? *Science* 335(6064): 20-22.

Epstein, G.L. (2008). The challenges of developing synthetic pathogens*. Bulletin of the Atomic Scientists*, available at: http://www.thebulletin.org/web-edition/features/the-challenges-of-developing-synthetic-pathogens.

Ericson, R.V. and Haggerty, K.D (1997). *Policing the Risk Society*. New York: Oxford University Press.

Ericson, R. V. and Doyle, A. (2004). *Uncertain Business: Risk, Insurance and the Limits of Knowledge*. Toronto: University of Toronto Press.

ETC Group (2007). *Extreme genetic engineering: An introduction to synthetic biology*, available at: https://www.cbd.int/doc/emerging-issues/etcgroup-introduction-synthetic-biology-2011-013-en.pdf.

Ewald, F. (1990). Norms, discipline and the law. *Representations* 30: 138-161.

Ewald, F. (1991). Insurance and risk. In: G. Burchell, C. Gordon and P. Miller (eds.) *Foucault effect: Studies in governmentality*. Chicago: University of Chicago Press.

Ewald, F. (2000). Risk in contemporary society. *Connecticut Insurance Law Journal* 6(2): 365-379.

Ewald, F. (2002). The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution. In: T. Baker and J. Simon (eds.) *Embracing Risk: the changing culture of insurance and responsibility*. Chicago: The University of Chicago Press.

Falkow, S. (2012). The lessons of Asilomar and the H5N1 "affair". *mBio* 3(5): 1-3.

Fearnley, L. (2008). Redesigning Syndromic Surveillance for Biosecurity. In: A. Lakoff and S.J. Collier (eds.) *Biosecurity Interventions: Global Health and Security in Question*. New York: Columbia University Press.

Fischer, M. and Maurer, S.M. (2010). Harmonizing biosecurity oversight for gene synthesis. *Nature Biotechnology* 28(1): 20-22.

Fisher, E. (2010). Risk regulatory concepts and the law. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Flick, U., von Kardorff, E., Steinke, I. (eds). (2004) *A companion to qualitative research*. London: Sage Publications Ltd.

Flick, U. (2004). Design and process in qualitative research. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Flick, U. (2004). Triangulation in qualitative research. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Flick, U. (2009). *An introduction to qualitative research* 4th edition. London: Sage Publications Ltd.

Furedi, F. (2009). Precautionary culture and the rise of possibilistic risk assessment. *Erasmus Law Review* 2(2): 197-220.

Garfinkel, M.S., Endy, D., Epstein, G.L. and Friedman, R.M. (2007). *Synthetic Genomics: Options for Governance*, available at: http://www.jcvi.org/.

Garfinkel, M.S., Endy, D., Epstein, G.L, and Friedman, R.M. (2008). Synthetic Biology. In: M. Crowley (ed.) *From Birth to Death and Bench to Clinic: The Hastings Center Bioethics Briefing Book for Journalists, Policymakers, and Campaigns*. Garrison, NY: The Hastings Center.

Garrett, L. (2012). Flu Season. *Foreign Policy* 5 January 2012, available at: http://www.foreignpolicy.com/articles/2012/01/05/flu_season?wp_login_redirect=0.

Giddens, A. (1990). *The consequences of modernity*. Stanford: Stanford University Press.

Gorman, B.J. (2006). Biosecurity and Secrecy Policy: Problems, Theory, and a Call for Executive Action. *Journal of Law and Policy* 2(1): 53-102.

Gottron, F. and Shea, D.A. (2011). *Federal Efforts to Address the Threat of Bioterrorism: Selected Issues and Options for Congress*. Congressional Service Report for Congress, 8 February, available at: http://www.fas.org/sgp/crs/terror/R41123.pdf.

Gottweis, H. (1998). *Governing Molecules: The Discursive Politics of Genetic Engineering in Europe and the United States*. United States of America: MIT Press.

Goulder, L.H. and Parry, I.W.H. (2008). Instrument Choice in Environmental Policy. *Review of Environmental Economics and Policy* 2(2): 152–174.

Graham, D.J. (2010). Why governments need guidelines for risk assessment and risk management. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Hacking, I. (1990). *The Taming of Chance*. Cambridge: Cambridge University Press.

Hacking, I. (1999). *The social construction of what?* Cambridge, MA: Harvard University Press.

Hacking, I. (2002). *Historical Ontology*. Cambridge, MA: Harvard University Press.

Harris, E.D. and Steinbruner, J. D. (2005). Scientific openness and national security after 9-11. *The CBW Conventions Bulletin* 67(March): 1-6.

Herfst, S. et al. (2012). Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets. *Science* 336(6088): 1534-1541.

Hermanns, H. (2004). Interviewing as an activity. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Heyl, B.S. (2001). Ethnographic interviewing. In: P. Atkinson, A. Coffey, S. Delamont, J. Lofland and L. Lofland (eds.) *Handbook of ethnography*. London: Sage Publications.

Hilgartner, S. (1992). The social construction of risk objects: Or, how to pry open networks of risk. In: J.F. Short, Jr. and L. Clarke (eds.) *Organizations, uncertainties and risk*. Boulder: Westview Press.

Hilgartner, S. (2007). Making the bioeconomy measurable: Politics of an emerging anticipatory machinery. *Biosocieties* 2(3): 381–389.

Holling, C.S. and Meffe, G.K. (1996). Command and Control and the Pathology of Natural Resource Management. *Conservation Biology* 10: 328–337.

Hood, C., Rothstein, H. and Baldwin, R. (2001). *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

Hopf (2004). Qualitative interviews: An overview. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Hutter, B.M. (2005). *The attractions of risk-based regulation: Accounting for the emergence of risk ideas in regulation*. Discussion Paper No. 33. Published by the Centre for Analysis of Risk and Regulation at the London School of Economics and Political Science, available at: http://www.lse.ac.uk/accounting/CARR/pdf/DPs/Disspaper33.pdf.

Hutter, B. and Power, M. (eds.) (2005). *Organizational Encounters with Risk.* Cambridge: Cambridge University Press.

Imai, M. et al. (2012). Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. *Nature* 486(21 June 2012): 420–428.

Implementation Support Unit of the Biological Weapons Convention. 'Biosafety and 'Biosecurity', an explanatory document prepared for BWC States Parties, available at: http://www.unog.ch/80256EDD006B8954/(httpAssets)/46BE0B4ACED5F0E0C125747B004F447E/$file/biosafety%2Bbackground%2Bpaper%2B-%2Badvanced%2Bcopy.pdf.

International Association Synthetic Biology (2009). *The IASB Code of Conduct for Best Practices in Gene Synthesis*, available at: http://www.ia-sb.eu/tasks/sites/synthetic-biology/assets/File/pdf/iasb_code_of_conduct_final.pdf.

International Committee of the Red Cross (2004). *Responsibilities of Actors in the Life Sciences to Prevent Hostile Use*, 20 January 2004, available at: http://www.icrc.org/eng/resources/documents/misc/5vdjlw.htm.

International Gene Synthesis Consortium (2009). *Harmonized screening protocol: Gene Sequence & Customer Screening to Promote Biosecurity*, available at: http://www.genesynthesisconsortium.org/wp-content/uploads/2012/02/IGSC-Harmonized-Screening-Protocol1.pdf.

International Risk Governance Council (2009). *Concept Note: Risk Governance of Synthetic Biology*. Risk Governance Council, Geneva, available at: http://www.irgc.org/IMG/pdf/IRGC_Concept_Note_Synthetic_Biology_191009_FINAL.pdf.

Irwin, A., Rothstein, H., Yearley, S. and McCarthy, E. (1997). Regulatory science: Towards a sociological framework. *Futures* 29(1): 17-31.

Jackson, R.J., Ramsay, A.J., Christensen, C.D., Beaton, S., Hall, D.F. and Ramshaw, I.A. (2001). Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. *Journal of Virology* 75(3): 1205-1210.

Jasanoff, S. (1987). Contested Boundaries in Policy-Relevant Science. *Social Studies of Science* 17(2): 195-230.

Jasanoff, S. (1990). *The Fifth Branch: Science Advisors as Policymakers*. Cambridge, MA: Harvard University Press.

Jasanoff, S. (1993). Bridging the two cultures of risk analysis. *Risk Analysis* 13(2): 123–129.

Jasanoff, S. (1995). Procedural choices in regulatory science. *Technology in Society* 17(3): 279-293.

Jasanoff, S. (2003a). Breaking the waves in science studies: Comment on H.M. Collins and Robert Evans, 'The Third Wave of Science Studies'. *Social Studies of Science* 33(3): 389-400.

Jasanoff, S. (2003b). (No?) Accounting for expertise. *Science and Public Policy* 30(3): 157–162.

Journal Editors and Authors Group. (2003). Statement on the consideration of biodefence and biosecurity. *Nature* 421: 771.

Kates, R.W. and Kasperson, J.X. (1983). Comparative risk analysis of technological hazards. *Proceedings of the National Academy of Sciences of the United States of America* 80: 7027-7038.

Kelle, A. (2007): *Synthetic biology and Biosecurity Awareness in Europe*, Bradford Science and Technology Report No.9, November 2007, available at: http://www.synbiosafe.eu/uploads///pdf/Synbiosafe-Biosecurity_awareness_in_Europe_Kelle.pdf.

Kelle, A. (2009). Ensuring the security of synthetic biology – towards a 5P governance strategy. *Systems and Synthetic Biology* 3(1-4): 85–90.

Kitsuse, J.I. and Spector, M. (1973). Toward a sociology of social problems: Social conditions, value-judgments, and social problems. *Social Problems* 20(4): 407-419.

Knight, F.H. (1921). *Risk, uncertainty and profit*. Boston and New York: Houghton Mifflin Company.

Kwik, G., Fitzgerald, J., Inglesby, V. and O'Toole, T. (2003). Biosecurity: Responsible Stewardship of Bioscience in and Age of Catastrophic Terrorism. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 1(1): 27-34.

Kwok, R. (2010). Five hard truths for synthetic biology. *Nature* 463: 288-290.

Lakoff, A. (2006). Preparing for the next emergency. Working Paper Laboratory for the Anthropology of the Contemporary, 19 January 2006.

Lakoff, A. and Collier, S.J. (eds.) (2008). The Problem of Securing Health. *Biosecurity Interventions: Global Health and Security in Question*. New York: Columbia University Press.

LaVan, D.A. and Marmon, L.M. (2010). Safe and effective synthetic biology. *Nature Biotechnology* 28(10): 1010–1012.

Ledford, H. (2010). Gene-synthesis rules favour convenience. *Nature* 467: 898, published online 18 October 2010, available at: http://www.nature.com/news/2010/101018/full/467898a.html.

Leitenberg, M. (2005). *Assessing the biological weapons and bioterrorism threat*, December 2005, available at: http://downloads.rjgodlewski.com/AssessingBioThreats.pdf.

Lempinen, E.W. (2011). "FBI, AAAS Collaborate on Ambitious Outreach to Biotech Researchers and DIY Biologists", available at: http://www.aaas.org/news/fbi-aaas-collaborate-ambitious-outreach-biotech-researchers-and-diy-biologists.

Lentzos, F. (2007). Representation from the trenches: Ongoing monitoring for implementing the BWC. *Disarmament Diplomacy*, available at: http://acronym.org.uk/dd/dd85/85bwc.pdf.

Lentzos, F. (2009). Synthetic Biology in the Social Context: The UK Debate to Date. *BioSocieties* 4: 303–315.

Lincoln, Y.S. (2004). Norman K. Denzin: Life in transit. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Lipschutz, R.D. (ed.) (1995). *On Security*. New York: Columbia University Press.

Lipschutz, R.D. and Turcotte, H. (2005). Duct Tape or Plastic? The Political Economy of Threats and the Production of Fear. In: B. Hartmann, B. Subramaniam, and C. Zerner (eds.) *Making Threats: Biofears and Environmental Anxieties*. Maryland: Rowman & Littlefield Publishers, Inc.

Lloyd's Emerging Risks Team (2009). *Synthetic Biology: Influencing Development*. Lloyd's Emerging Risks Team Report, available at: http://www.lloyds.com/~/media/25352cf96fee4a8fb28f4ab1746f58ac.ashx.

Loasby, B.J. (1976). *Choice, complexity, and ignorance*: *An enquiry into economic theory and decision-making*. London: Cambridge University Press.

Luhmann, N. (1993). *Risk: A sociological theory*. New York: Transaction Publishers.

Lynch, D. and Vogel, D. (2001). The Regulation of GMOs in Europe and the United States: A Case-Study of Cotemporary European Regulatory Politics. *Council on Foreign Relations*, 5 April 2001, available at: http://www.cfr.org/genetically-modified-organisms/regulation-gmos-europe-united-states-case-study-contemporary-european-regulatory-politics/p8688.

Machi, E. and McNeill, J.B. (2010). New Technologies, Future Weapons: Gene Sequencing and Synthetic Biology. *Homeland Security 2020* No. 2 24 August 2010, available at: http://thf_media.s3.amazonaws.com/2010/pdf/wm2986.pdf.

Majone, G. (2010). Strategic Issues in Risk Regulation and Risk Management. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Malakoff, D. and Enserink, M. (2012). In Dramatic Move, Flu Researchers Announce Moratorium on Some H5N1 Flu Research, Call for Global Summit. *ScienceInsider*, 20 January 2012, available at: http://news.sciencemag.org/scienceinsider/2012/01/in-dramatic-move-flu-researchers.html.

Malakoff, D. (2013). H5N1 Researchers Announce End of Research Moratorium. *Science*Insider, 23 January 2013, available at: http://news.sciencemag.org/scienceinsider/2013/01/h5n1-researchers-announce-end-of.html http://news.sciencemag.org/scienceinsider/2013/01/h5n1-researchers-announce-end-of.html.

Maurer, S.M. and Zoloth, L. (2007). Synthesizing biosecurity. *Bulletin of the Atomic Scientists* 63(6): 16-18.

Maurer, S.M. (2010). Beyond Treaties and Regulation: Using Market Forces to Control Dual Use Technologies. Goldman School of Public Policy Working Paper No. GSPP10-010, 1 November 2010, available at: http://dx.doi.org/10.2139/ssrn.1705630.

Maurer, S.M. (2011). The End of the Beginning or the Beginning of the End? Synthetic Biology's Stalled Security Agenda and the Prospects for Restarting It. *Valparaiso University Law Review* 45(4): 73-132.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations* 14(4): 563–587.

McLeish, C. and Nightingale, P. (2005). *The Impact of Dual Use Controls on UK Science: Results From a Pilot Study*. SPRU Electronic Working Paper Series. Paper No. 132.

McLeish, C. and Nightingale, P. (2007). Biosecurity, bioterrorism and the governance of science: The increasing convergence of science and security policy. *Research Policy* 36: 1635–1654.

Merkens, H. (2004). Selection procedures, sampling, case construction. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Miller, P. and Rose, N. (1990). Governing economic life. *Economy and Society* 19(1): 1-31.

Moodie, M. (2009). Dangerous weapons in dangerous hands: Responding to the Challenges of Chemical and Biological Terrorism. *Proliferation Papers*, in collaboration with the Atomic Energy Commission, Summer 2008, available at: http://www.ifri.org/?page=contribution-detail&id=5389&id_provenance=97.

Mukunda, G., Oye, K.A. and Mohr, S.C. (2009). What Rough Beast? Synthetic biology, uncertainty, and the future of biosecurity. *Politics & Life Sciences* 28(2): 2-26.

National Academy of Sciences (1982). *Scientific Communication and National Security*. Washington, DC: National Academy Press.

National Institutes of Health (2011). *NIH Guidelines for Research Involving Recombinant DNA Molecules* October 2011, available at: http://oba.od.nih.gov/oba/rac/guidelines/nih_guidelines.pdf.

National Research Council (1983). *Risk Assessment in the Federal Government: Managing the Process*. Washington, DC: The National Academies Press.

National Research Council (1989). *Field Testing Genetically Modified Organisms: Framework for Decisions.* Washington, DC: The National Academies Press.

National Research Council (1996). *Understanding Risk: Informing Decisions in a Democratic Society*. Washington, DC: The National Academies Press.

National Research Council (2004). *Biotechnology Research in an age of terrorism: Confronting the dual use dilemma*. Washington, DC: The National Academies Press.

National Research Council (2006) *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington, DC: The National Academies Press.

National Research Council (2007). *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*. Washington, DC: The National Academies Press.

National Research Council (2008). *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change*. Washington, DC: The National Academies Press.

National Research Council (2010). *Sequence-Based Classification of Select Agents: A Brighter Line*. Washington, DC: The National Academies Press.

National Research Council (2011). *Life Science and Related Field: Trends in Science and Technology Relevant to the Biological Weapons Convention*. Washington, DC: The National Academies Press.

National Science Advisory Board for Biosecurity (2006). *Addressing biosecurity concerns related to the synthesis of Select Agents*. Report of the National Science Advisory Board for Biosecurity (NSABB) December 2006.

National Science Advisory Board for Biosecurity (2007). *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information*. Report of the National Science Advisory Board for Biosecurity (NSABB) June 2007.

National Science Advisory Board for Biosecurity (2008). *Strategic Plan for Outreach and Education On Dual Use Research Issues*. Report of the National Science Advisory Board for Biosecurity (NSABB) 10 December 2008.

National Science Advisory Board for Biosecurity (2010). *Addressing biosecurity concerns related to synthetic biology*. Report of the National Science Advisory Board for Biosecurity (NSABB) April 2010.

National Science Advisory Board for Biosecurity (2011). *Strategies to Educate Amateur Biologists and Scientists in Non-life Science Disciplines About Dual Use Research in the Life Sciences*. Report of the National Science Advisory Board for Biosecurity (NSABB) June 2011.

National Science Advisory Board for Biosecurity (2012). *Findings and Recommendations*, 29-30 March 2012, available at: http://oba.od.nih.gov/oba/biosecurity/PDF/03302012_NSABB_Recommendations.pdf.

National Security Decision Directive 189. 21 September 1985, available at: http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

Nature (2006). Editorial: Towards better biosecurity. *Nature* 440(7085): 715.

Nature Biotechnology (2009). News Feature: What's in a name? *Nature Biotechnology* 27(12): 1071-1073.

Nexon, E. (2011). Strengthening the BTWC through laboratory best practices and biosecurity. *Non-Proliferation Papers* No. 3 December 2011, available at: http://www.nonproliferation.eu/documents/nonproliferationpapers/elisandenexon4ed77d757f975.pdf.

Nixdorff, K., Davison, N., Millett, P. and Whitby, S. (2008). *Technology and Biological Weapons: Future Threats*. Science and Technology Report No. 2.

Office of Science Technology and Policy (1986). *Coordinated Framework for Regulation of Biotechnology* 51 Fed. Reg. 23 302 (26 June).

O'Malley, P. (1992). Risk, power and crime prevention. *Economy and Society* 21(3): 252-275.

O'Malley, P. (2000). Uncertain subjects: risks, liberalism and contract. *Economy and Society* 29(4): 460-484.

O'Malley, P. (2003). Governable catastrophes: a comment on Bougen. *Economy and Society* 32(2): 275-279.

O'Malley, P. (2004). *Risk, Uncertainty and Government*. London: Glasshouse Press.

Organisation for Economic Co-operation and Development (2010). *Risk and Regulatory Policy: Improving the Governance of Risk*. OECD Publishing, Paris.

Parliamentary Office of Science and Technology (2008). *POSTNOTE: Synthetic Biology*, available at: http://www.parliament.uk/documents/post/postpn298.pdf.

Pearson, G.S. (1993). Prospects for Chemical and Biological Arms Control: The Web of Deterrence. *Washington Quarterly* 16(2): 145-162.

Petro, J.B., Plasse, T.R. and McNulty, J.A. (2003). Biotechnology: Impact on Biological Warfare and Biodefense. *Biosecurity and Bioterrorism: Biodefense Strategy, Practices and Science* 1(3): 161-168.

Pfadenhauer, M. (2009). At eye level: The expert interview – a talk between expert and quasi-expert. In: A. Bogner, B. Littig and W. Menz (eds.) *Interviewing Experts*. Basingstoke England: Palgrave Macmillan.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos.

Power, M. (2005). The invention of operational risk. *Review of International Political Economy* 12(4): 577–599.

Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford and New York: Oxford University Press.

Power, M., Scheytt, T., Soin, K. and Sahlin, K. (2009). Reputational Risk as a Logic of Organizing in Late Modernity. *Organization Studies* 30(2-3): 301-324.

Power, M. (2013). The apparatus of fraud risk. *Accounting, organizations and society* 38(6–7): 525–543.

Presidential Commission for the Study of Bioethical Issues (2010). *New Directions: The Ethics of Synthetic Biology and Emerging Technologies*. Washington, DC, December 2010, available at: http://bioethics.gov/sites/default/files/PCSBI-Synthetic-Biology-Report-12.16.10.pdf.

Purnick, R.E.M. and Weiss, R. (2009). The second wave of synthetic biology: From modules to systems. *Nature Reviews* 10(June): 410-422.

Rabinow, P. (2008). Episodes or Incidents: Seeking Significance. In: A. Lakoff and S.J. Collier (eds.) *Biosecurity Interventions: Global Health and Security in Question*. New York: Columbia University Press.

Rains, P. (1975). Imputations of deviance: A retrospective essay on the labeling perspective. *Social Problems* 23(1): 1-11.

Rappert, B. (2003). Biological weapons, genetics, and social analysis: Emerging responses, emerging issues-II. *New Genetics and Society* 22(3): 297-314.

Rasmussen, S. et al. (2004). Transitions from nonliving to living matter. *Science* 303(5660): 963-965.

Relman, D.A., Choffnes, E. and Lemon, S.M. (2006). In search of biosecurity. *Science* 311: 1835.

Relman, D.A. (2010). The biological century: coming to terms with risk in the life sciences. *Nature Immunology* 11(4): 275-278.

Relyea, H.C. (2003). Government secrecy: Policy depths and dimensions. *Government Information Quarterly* 20: 395-418.

Reppy, J. (2003). Regulating Biotechnology in the Age of Homeland Security. *Science Studies* 16(2): 38-51.

Rhodes, R.A.W. (1996). The new governance: Governing without government. *Political Studies* XLIV: 652-667.

Roberts, A. (2006). *Blacked Out: Government Secrecy in the Information Age*. Cambridge: Cambridge University Press.

Rose, N. (2000). Government and control. *British Journal of Criminology* 40: 321-339.

Rose, N. (2001). The politics of life itself. *Theory, culture and society* 18: 1-30.

Rose, N. (2002). At Risk of Madness. In: T. Baker and J. Simon (eds.) *Embracing Risk: the changing culture of insurance and responsibility*. Chicago: The University of Chicago Press.

Rothstein, H., Huber, M. and Gaskell, G. (2006). A theory of risk colonization: the spiralling regulatory logics of societal and institutional risk. *Economy and Society* 35(1): 91-112.

Samuel, G.N., Selgelid, M.J. and Kerridge, I. (2009). Managing the unimaginable: Regulatory responses to the challenges posed by synthetic biology and synthetic genomics. *EMBO Reports* 10(1): 7-11.

Schmidt, M. (2008). Diffusion of synthetic biology: a challenge to biosafety. *Systems and Synthetic Biology* 1(1-2): 1-6.

Schmidt, M. and Giersch, (2011). DNA synthesis and security. In: M.J. Campbell (ed.) *DNA Microarrays, Synthesis and Synthetic DNA*. United States: Nova Science Publishers Inc.

Schneider, J.W. (1985). Social problems theory: The constructionist view. *Annual Review of Sociology* 11(1985): 209-229.

Selgelid, M.J. (2007). Ethics, Bioterrorism, and the Censorship of Science. *Hastings Center Report* May-June: 35-43.

Selgelid, M.J. (2009). Governance of dual-use research: An ethical dilemma. *Bulletin of the World Health Organization* 87(9): 720-723.

Short, J.F. Jr. (1984). The Social Fabric at Risk: Toward the Social Transformation of Risk Analysis. *American Sociological Review* 49(December): 711-725.

Smith, G.L. and Davison, N. (2010). Assessing the spectrum of biological risks. *Bulletin of the Atomic Scientists* January/February 2010: 1-11.

Smithson, A.E. (2010). Pathogens and Arms Control: Can Bioscience Police Itself? *Survival* 52(5): 117-134.

Somerville, M.A. and Atlas, R.M. (2005). Ethics: A Weapon to Counter Bioterrorism. *Science* 307(5717): 1881-1882.

Starr, C. (1969). Social Benefit versus Technological Risk: What is our society willing to pay for safety? *Science* 165: 1232-1238.

Steinbruner, J., Harris, E.D., Gallagher, N. and Okutani, S.M. (2007). *Controlling Dangerous Pathogens: A Prototype Protective Oversight System*. The Center for International and Security Studies at Maryland, available at: http://www.cissm.umd.edu/papers/files/pathogens_project_monograph.pdf.

Stirling, A. and Mayer, S. (2001). A novel approach to the appraisal of technological risk: A multicriteria mapping study of a genetically modified crop. *Environment and Planning C: Government and Policy* 19: 529-555.

Stirling, A. (2010). Keep it Complex. *Nature* 468(23 December 2010): 1029-1031.

Suk, J.E. et al. (2011). Dual-Use Research and Technological Diffusion: Reconsidering the Bioterrorism Threat Spectrum. *PLoS Pathogens* 7(1): 1-3.

Tait, J. (2009). Upstream engagement and the governance of science. *EMBO Reports* 10(1S): S18-S21.

Tierney, K.J. (1999). Toward a Critical Sociology of Risk (1999). *Sociological Forum* 14(2): 215-242.

Torgersen, H. (2009). Synthetic biology in society: learning from past experience? *Systems and Synthetic Biology* 3:9-17.

Tucker, J.B. and Zilinskas, R.A. (2006). The Promise and Perils of Synthetic Biology. *The New Atlantis* Spring 2006: 24-45.

Tucker, J.B. (2011). Could Terrorists Exploit Synthetic Biology? *The New Atlantis* Spring 2011: 69-81.

Tumpey, T.M. et al. (2005). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science* 310(5745): 77-80.

Van Munster, R. (2005). Logics of security: The Copenhagen School, risk management and the war on terror. University of Southern Denmark: Political Science Publications, available at: http://static.sdu.dk/mediafiles/Files/Om_SDU/Institutter/Statskundskab/Skriftserie/05RVM10.pdf.

Vastag, B. (2003). Openness in Biomedical Research Collides With Heightened Security Concerns. *Journal of the American Medical Association* 289(6): 686-690.

Vogel, K.M. (2008a). Biodefense: Considering the sociotechnical dimension. In: A. Lakoff and S.J. Collier *Biosecurity Interventions: Global Health and Security in Question*. New York: Columbia University Press.

Vogel, K.M. (2008b) 'Iraqi Winnebagos™ of death': Imagined and realized futures of US bioweapons threat assessments. *Science and Public Policy* 35(8): 561–573.

Vogel, K. (2008c). Framing biosecurity: an alternative to the biotech revolution model? *Science and Public Policy* 35(1): 45-54.

Wæver, O. (1995). Securitization and Desecuritization. In: R.D. Lipschutz (ed.) *On Security*. New York: Columbia University Press.

Weinberg, A. (1972). Science and trans-science. *Minerva* 10(2): 209-222.

Weinberg, A. (1985). Science and its limits: The regulator's dilemma. *Issues in Science and Technology* 2(1): 59-72.

Weingart, P. (1999). Scientific expertise and political accountability: Paradoxes of science in politics. *Science and Public Policy* 26(3): 151-161.

Wiener, J.B. (2010). Risk regulation and governance institutions. In: OECD *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Wilkinson, I. (2010). *Risk, Vulnerability and Everyday Life*. Oxon: Routledge.

Wilsdon, J. (2004). The politics of small things: Nanotechnology, risk, and uncertainty. *Technology and Society Magazine* 23(4): 16-21.

Wimmer E., Mueller S., Tumpey, T.M. and Taubenberger J.K. (2009). Synthetic viruses: A new opportunity to understand and prevent viral disease viral disease. *Nature Biotechnology* 27(12): 1163-1171.

Wolff, S. (2004). Analysis of documents and records. In: U. Flick, E. von Kardorff and I. Steinke (eds.) *A companion to qualitative research*. London: Sage Publications Ltd.

Wolt, J.D. and Peterson, R.K.D. (2000). Agricultural biotechnology and societal decision-making: The role of risk analysis. *AgBioForum* 3(1): 39-46.

World Health Organization (2006). *Biorisk management: Laboratory biosecurity guidance*, available at: http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf.

World Health Organization (2012). *Report on technical consultation on H5N1 research issues*, Geneva, 16–17 February 2012, available at: http://www.who.int/influenza/human_animal_interface/mtg_report_h5n1.pdf.

Wright, S. (1986). Molecular Biology or Molecular Politics? The Production of Scientific Consensus on the Hazards of Recombinant DNA Technology. *Social Studies of Science* 16(4): 593-620.

Wright, S. (2004). Taking biodefense too far. *Bulletin of Atomic Scientists* 60(6): 58-66.

Wright, S. (2007). Terrorists and biological weapons: Forging the linkage in the Clinton Administration. *Politics and the Life Sciences* 25(1-2): 57-115.

Zilinskas, R.A. and Tucker, J.B. (2002). Limiting the contribution of the open scientific literature to the biological weapons threat. *Journal of Homeland Security*, December 2002.

Zinn, J.O. (2004). *Literature review: Sociology and risk*. Social Contexts and Responses to Risk Network (SCARR). Working Paper 2004/1.