# GREEN PAPER:

## **Safety, Security, Preparedness:**
## An Orientation to Biosecurity Today

Stavrianakis, Fearnley, Bennett, Rabinow[1]

We argue that today we are confronted by a distinctive biosecurity problem. This problem, although connected to the work and formulations of the Asilomar conference on recombinant DNA and the Biological Weapons Convention in February and March 1975 respectively (Berg et al. 1975; Singer and Berg 1976), nonetheless is characterized by significant discontinuities. Three vectors are particularly significant. First, there have been technical innovations since the 1970s, including, but not limited to, synthesis technologies (Bugl et al. 2007). Second, there have been changes in the political milieu, including the emergence of non-state terrorism at a global scale (Alibek 1999; Laquer 2003; Dando 2006). Third, the rise of new security frameworks within government apparatuses are increasingly to "low-probability/high-consequence" events rather than civil defense and all-hazards planning (Collier and Lakoff 2008). These three vectors provide preliminary orientation for an analysis of the problem of biosecurity today.

Given these vectors, as well as others, we propose that a sufficient analysis of biosecurity today requires not only attention to specific safety techniques and regulatory policies, but additionally, the rationalities according to which practices and resources are being mobilized today. In this paper we will devote our attention to distinguishing and characterizing three types of rationalities: ***safety, security,*** and ***preparedness***. By so doing, we argue that we can facilitate a better analysis of what currently is taken to count as a security problem.

Our analysis arises in part from our position within the Berkeley Human Practices Laboratory. For five years (2006-2011) Rabinow and Bennett experimented with collaboration between science and ethics as a core research component of an NSF funded Synthetic Biology Engineering Research Center (SynBERC). They call this effort "Human Practices" (Rabinow and Bennett 2011). The Human Practices thrust of SynBERC focused on the challenge of bringing biosciences and human sciences into a collaborative relationship, on common problems, such as biosecurity. In this Green Paper, we reflect on the extent to which SynBERC, as an organization, is prepared for the challenges of the security environment in which practices of bio-engineering exist.

**Safety**

The relation between technical innovation and the expansion of danger in biotechnology has long been framed as an issue of safety, which can be addressed through technical solutions. The emphasis is on prevention and protection. As a technical term, "safety" means addressing dangers through safeguards and procedures. These measures are

valuable as far as they go. However ready access to the know-how if not the materials and technologies of DNA synthesis pose limits to a safeguards approach. Neither challenges related to new political environments, nor challenges introduced by indetermination can be adequately addressed through a mode of safety.

We distinguish two different approaches to safety. The first, "safety-by-design," consists of a strategy to modify genomes in a designed manner in order to anticipate and prevent negative ramifications. A privileged example of this approach is the work of George Church, Professor of Genetics at Harvard Medical School, and one of the instigators of the Human Genome Project. Professor Church is a Principal Investigator for the "chassis" work being done within SynBERC. "Chassis" here refers to redesigned cells and genomes capable of housing and acting as 'power supplies' sustaining proper functioning for designed biological systems. One of the principle safety challenges with regards to this work is the fact that these proposed re-engineered cells will integrate with the ecosystem. The challenge is to design 'safe' chasses that will not cause ecological disasters. Church argued that his approach circumvents the precautionary principle, widely accepted in Europe, by designing new nucleotides not found in nature. By so doing Church claims that organisms containing these nucleotides will not be able to propagate outside of the lab (Church 2005).

A second approach to safety turns on regulatory mechanisms (Cook-Deegan et al. 2005). This approach is exemplified by researchers at the UC Berkeley Goldman School of Public Policy (Maurer et al 2006). A whitepaper published by this group, "From Understanding to Action: Community-Based Options for Improving Safety and Security in Synthetic Biology," attempts to extend the proceeduralist approach characteristic the 1975 Asilomar convention. This approach is a mixture of technical criticism and what some have called "science and society" (Nowotny et al 2001). The report suggests that 'self-governance' is a preferable mode of governance compared to outside regulation. The most significant aspect of the report is the use of the Asilomar conference as the gold standard of such self-governance.

In this proceeduralist framing, moving from knowledge to action requires consensus and agreement on what is deliverable before action can be executed. The assumption behind this relationship of knowledge and action is that things people reliably know are adequate for action and regulation. The position that suggests knowledge about how to self-govern is axiomatic comes from a model developed in the 70s at Asilomar when biotechnology was reacting for the first time to wider concerns regarding safety and security of the emerging field. If the 'how' of governance is already known, then what is needed is information to be collected on possible interventions, voted on and implemented. The limitation of this mode is that regulatory mechanisms are ill-designed to take up emerging dangers generated by enhanced capacities. We wish to pose as an open question whether and in what way enhanced capacities change both the object and form of governance at stake in a global political milieu. Both proceduralism and safety-by-design are attempts to extend self-governance models developed by the Asilomar conference on recombinant DNA and its successors. The scientific, industrial, and political milieus today are strikingly different. Given the internet and the globalization of science, access to materials and specialized knowledge is widespread. As such, the technical safeguards being developed by those designing genomes can only have limited efficacy. Let us be clear, there are problems for which technical safeguards and community procedures are sufficient responses. On the whole, for instance, laboratory safety procedures work. However, the key externality of this rationality is that it can only address those aspects of the security challenge that are amenable to technological safeguards and procedures.

A current critical limitation of efforts in both safety-by-design as well as proceduralism is that these efforts conflate and thereby obscure the distinctiveness of problems of ***security*** as opposed to problems of ***safety***. An example of a safety problem conflated with a problem of security is dual-use. The assumption that bad actors using technologies for nefarious purposes can be comprehensively addressed through technical safeguards and procedures of self-governance is misleading. This conflation is taken to call for a technological response by existing specialists: can a biological chassis be designed in such a way that it cannot be subsequently "misused"? It is also taken to call for the formalization of the community of synthetic biology practitioners: can a formalized association develop procedures for self-governance that would screen out potentially nefarious actors?

It is clear that there are problems of laboratory and environmental safety that demand technological and procedural responses. It is also clear that these responses can play a minor role in formulating safeguards for wider security challenges. Problems and practices connected to a rationality of safety, however, become critical limitations when overextended. Thus, when it is held that the salient security challenges can be mitigated adequately through technical means, police procedures among and between labs, and trust in the expertise and character of current specialists, a critical limitation has been obscured.

Claim: technical safeguards can deliver on security

1. First outside: insufficient technical **standards**
2. Second outside: the security questions are obscured by the safety proceedures such that it appears as though security is being addressed

## Security

In the US and elsewhere, the post-9/11 political environment is characterized by two sets of distinct challenges: (1) a new range of actors and actions, and (2) the internet and other new media provide global access to technological know-how and scientific knowledge. Such global access cannot be addressed using existing models of nation-specific nor international regulation and therefore calls for the invention of new platforms of security. Whereas a safety platform operates within a logic of technological safeguards, a security platform additionally concerns challenges related to political environment. The major externality of security as a platform for addressing the concerns of the global political milieu is that it does not focus on preparation for low probability, high consequence events, as we will note in the next section.

Policy work, including proposals by the Sloan Foundation (Garfinkel et al. 2007) , National Research Council (aka the "Fink" Report) (NRC 2004), the National Science Advisory Board for Biosecurity (NSABB 2007) and the Industry Association Synthetic Biology (IASB 2008) recognizes the political milieu as the context in which research operates and explicitly attempt to address this as a problem. We distinguish this as a mode of security. Often the security milieu as a challenge is framed in such a way that a safety platform becomes the solution to such a problem (IASB 2008).

While safety focuses on technical solutions, security aims to maximize the circulation of elements in a context of risk. The objective of a mode of security is thus not the prevention of specific dangers or the protection of specific spaces, but governance of a milieu in which the elements of the science circulate. This milieu is characterized by both risks and harms. The Sloan, Fink and NSABB reports frame the question of security in terms of the concept of 'dual-use research of concern'. In the report from June 2007 "A Proposed Framework for the Oversight of Dual Use Life Sciences Research" the NSABB developed a recommendation for a framework within which the government can develop a comprehensive system of

identification and review of dual use research. Dual use is identified as research with benevolent and malevolent "potential" applications. The general framework is to minimize risk of misuse and maximize open exchange of information.

The Sloan report "Synthetic Genomics: Options for governance" formulates governance options that attempt to minimize safety and security risks. The report focused on three main concerns: bioterrorism, worker safety and protection of communities and the environment outside of legitimate laboratories. Using the distinction between a mode of safety and a mode of security we can say that bioterrorism and the environment are vectors for which a platform of security is appropriate, while worker safety requires a safety platform. The Sloan report divides options for governance into three main categories: commercial synthesis companies, tools and reagents, users and organizations.

1. Options for synthesis companies focus on requiring commercial firms to use specific software to screen potential orders and those who order, comparing the sequence of submitted DNA orders to a list of known pathogens. The goal is to maximize the circulation of licit materials while minimizing the circulation of illicit materials.

2. Options for technology and reagents emphasize monitoring and controlling the circulation of DNA synthesizers. Methods include registration (a requirement to notify the government in the purchase, sale or possession of technology) and licensing (in which a government approved license is required for the purchase, sale or possession of technology).

3. Options for users and organizations remain in a mode of safety, focusing on 'best practices', IBC review, and education about risks.

While remaining in a mode of safety, the Sloan report options for users and organizations provokes thinking about pedagogy and preparedness. Alexander Kelle working within the EU SynBIOSAFE project took up this provocation (Kelle 2007). He quotes the British biosecurity scholar Malcom Dando when he suggests that based on responses from 1,600 life scientists during 60 seminars in 8 countries Dando concluded that life scientists "do not share the threat perception widespread among biosecurity experts concerning bioterrorism or biological warfare. They do not think that their own work might contribute to the threat. Life scientists have practically no knowledge of legally binding international regulatory instruments, such as the Biological Weapons Convention" (Kelle 2007, 13). Kelle's research shows just this, having conducted interviews with leading practitioners within synthetic biology on their awareness and knowledge of current efforts around the biosecurity challenge. It is significant that, for example, 13 of the 18 interviewed had not heard of the Fink report. The real question then is not just how to raise awareness of "issues" among scientists working within synthetic biology but how to make something as constitutive as the political ecology within which their science is being practiced a meaningful set of issues to engage with relative to their daily practice. The June 2007 NSABB report makes the important point that synthetic biology is one among a number of sub-disciplines within the life sciences which have to be brought within a more comprehensive approach to the challenge of biosecurity.

Reflecting on the work by Kelle and colleagues in Europe we see that there are not enough cases in synthetic biology through which probabilistic assessments can be made. Instead the method was to conduct interviews out of which to make judgments. As an approach this allows us to ask which capacities and deficiencies the community of researchers more broadly has. Specifically it showed our research group which areas were important to try and work on pedagogically within our research organization; namely, the

integration of capacity building relative to the security challenge into daily practice. This is a response to the provocation cited by Maclom Dando , after awareness raising, ‘then what?’ (Revill and Dando 2008). Our response to the question of ‘then what?’ was to tie awareness into the practice of science.

A central—though insufficiently examined—supposition of the expertise demonstrated, for instance, in the Sloan report, is that such experts are capable of conceptualizing dangers, both known and unknown, as risks that can subsequently be assessed with appropriate rigor and plausibility. This is what can be called “Mode One” expertise (Nowotny *et al* 2001). Mode One consists in inventory, consultation, and cooperation among experts. The core assumption—often taken for granted and not subject to scrutiny—is that the expertise of existing specialists in one domain is adequate without major adjustment to emerging problems. Mode One experts operate with a metric of certainty within an ever-receding zone of uncertainty. Uncertainty, however, does not undermine the decision making imperative of Mode One experts. Rather, this dynamic provides the motor of their legitimation. In our view, the existence of such a capability is very much in question.

Few deny that synthetic biology, to the extent that it makes biology easier to engineer, introduces new dangerous actions and actors into the post 9/11 political milieu. The question of whether or not, as of today, such dangers can be assessed as risks, however, remains an open one. That question depends in part on the ability of Mode One specialists to figure synthetic biology as a field of probabilities, conceptualized in a verificational mode, and made available to techniques of normalization.

Following Niklas Luhmann (Luhmann, 1993) it is useful to distinguish dangers from risks. Dangers are empirical factors that exist in the world in a scientifically under-examined state. Strictly speaking, dangers are inchoate in a veridictional sense, which is to say that they lack a conceptual structure to order them, and hence they do not operate in the domain of legitimate truth claims. It is only once dangers are conceptualized and enter into a grid of knowledge that technically they become risks. Risks, unlike dangers, can be scientifically assessed. The relative likelihood of a series unfolding in a particular manner can then be determined, and strategies for minimization and maximization elaborated.

There are, of course, different ways of thinking about dangers, and therefore different ways of turning them into risks. On the most refined readings, security related events in synthetic biology are conceived in terms of the ratio between probability and consequence. Events of interest are taken to be of low-probability but of high consequence. The question is: how is such a judgment made? How can it be known whether or not the probability of events is low or high? Such judgments, again strictly speaking, can only be made in relation to a multiplicity of actual events. It is only when there have been multiple events categorized and classified that they can be taken up as a series. It is in relation to this series that claims of probability can be systematically derived. This probabilistic mode arose from insurance in which long statistical series were established and from which probabilistic accounts were constructed. Specific sectors of these probabilistic series could then be assigned risk values and insurance premiums could be calculated.

Claim: security is produced through mechanisms to ensure correct circulation and through the naming of experiments of concern

1. First outside: dangers cannot be turned into risks, i.e. experts do not have norms for security

2. Second outside: experiments of concern are really experiments of reassurance not only do they not orient action toward preparing for unexpected events, but they block such efforts

## Preparedness

While some dangers are presently understood as risks (Douglas 1992; Luhmann 1993; Beck 1995), and can be calculated probabilistically, we lack platforms for confronting a range of new dangers which fall outside of previous categories and a probabalistic mode of reasoning (Ewald 2002). Such platforms would need to be characterized by vigilant observation, pedagogy, and adaptation (Lakoff 2008). As a technical term, preparedness is a way of thinking about and responding to significant problems whose impacts would have large-scale ramifications (e.g. a bioterrorist attack or the spread of a deadly virus), but whose probability cannot be feasibly calculated, and whose specific form cannot be determined in advance.

Safety is about designing rules or technologies that control behaviors and materials in order to reduce danger. Security operates on how such elements circulate in political milieu. Preparedness is not about the regulation or control of the object. It is about capacities for thinking about and responding to low probability high consequence events which are outside probabilistic modes of reason. There is no transformation of the danger into a calculable risk and in fact in many situations the form of the danger is bracketed (because by definition you cannot know it). As such, the work must be done on the capacities of response and recovery of the organizational form within which the individual researcher operates.

The NSABB suggests that while virtually all life sciences research has dual use potential the number of 'truly' dual use research of concern is minimal. Importantly they suggest that on the basis of this, "misuse of dual use research of concern is therefore a *low-probability high-consequence event*, and this is a significant factor in the NSABB's formulation of oversight recommendations" (NSABB 2007). This is obviously significant relative to the broader norm of preparedness emerging from US national security sites (Lakoff and Collier 2008). The NSABB then insists that the response should be to institute new biosecurity measures to minimize this *risk*, i.e. to minimize the probability of a low probability event taking place. They ignore the imperative to think about how to *prepare* for the ramifications of a high consequences event.

Both safety and security remain important aspects of a comprehensive approach to the governance of synthetic biology. However, today's singular conjuncture of emerging bio-technical capacities and globalizing political milieus pose problems that defy both *regulation* and *control*. As the NSABB report acknowledges, potential dangers include events that are of low-probability but high-consequence. Not only is the timing of a future event uncertain, the form it will take is by definition unknown. As such, these events cannot be transformed into calculable risks and normalized through apparatuses of security. Regulations aimed at known laboratories and known agents are equally insufficient. The threat of low-probability high-consequence events requires a turn toward a third mode of practice: *preparedness.*

In a series of recent papers, Collier and Lakoff trace the emergence of preparedness as a norm of rationality in U.S. government planning (Lakoff 2008, Collier and Lakoff 2008). Beginning with civil defense plans developed against the threat of nuclear attack in the 1950s, they argue that preparedness norms and techniques spread to a number of disparate domains. Preparedness plans are today applied to a wide range of emergencies, including natural disasters, disease outbreaks, and terrorist attacks. In fact, today preparedness is being reorganized as an "all-hazards" function, that is, a generic toolkit oriented towards emergency-scale events without reference to their specific cause.

Preparedness is not prediction. Rather than an attempt to define the form or content of the future, preparedness requires a turn toward work on capacities. Practices such as scenario-thinking and simulations employ "worst-case scenarios" in order to identify vulnerabilities, limitations and externalities. From this exercise better disaster responses can be worked on. For example, in early civil defense planning, simple 'blast grids' were overlaid on top of city maps in order to simulate the damage caused by a nuclear bomb. Using these simulated visions of the city allowed a novel mode of planning for future dangers. Rather than calculating and mapping risks, this technique highlighted vulnerabilities (which roads would be unusable? Which hospitals destroyed?) in order that improvements could be made. Improvements could take two paths: a focused enhancement of safety and security practices; or preparations for disaster response.

In a section of the 2007 report entitled "Need for engagement of the life sciences community" the NSABB names a number of key areas they want to see worked on; a culture of responsibility and three stakeholder areas, health, national security, vitality of the life sciences research enterprise. The report suggests that "responsible scientists have a duty to be aware of the potential for misuse of their scientific findings with dual use potential" (NSABB 2007, 12). What kind of responsibility is this? We suggest that this is not just a minimization of risk but a preparation for ramifications of events. At the level of the laboratory this might include engaging in pedagogical exercises or interfacing with local, national and international public health and security actors. What are the practices that are adequate to good research within this security milieu? The NSABB highlight an insight from the UK's Royal Society / Wellcome trust report from 2004 'Do no harm: Reducing the potential for the misuse of life science research' where they suggest that, "the challenge is to think beyond the obvious and identify those avenues of research and technologies that present risks of being misused for harmful purposes that are quite distinct from the original aims of the work. This needs *imaginative thinking* as the vast majority of work falls into the grey area of having some potential for misuse" (NSABB 2007, 13-14). This means both imaginative thinking relative to misuse and imaginative thinking relative to high consequence events.

As the NSABB go on to say, "the responsible conduct and communication of dual use research of concern depend largely on the individual conducting such activities. No criterion or guidance document can anticipate every possible situation" (NSABB 2007, 15). Responsibility does not mean only the individual capacity to minimize risk but also the capacity of individuals within organizational forms to respond to events. This is the norm of preparedness.

1. In synthetic biology and in SynBERC in particular, this hasn't been done
2. If this kind of exercise is engaged in, it must be asked: What are the externalities and critical limitations of exercises for preparedness such as scenario planning?

**Conclusion**

Current work at the interface of synthetic biology and security has identified three classes of problems: (1) the expansion of technical capacities; (2) challenges arising from the post-9/11 security environment, including new levels of access to materials and know-how, the globalization of biotechnology, and a new range of potentially malicious actors and actions; (3) preparedness for a low probability/high-consequent event, either accidental or malicious.

Sustained attention has been given to addressing the first class of problems within a *safety* framework in which dangers are confronted with technical safeguards (e.g. the Sloan Report). The second class has been addressed in broad terms by folding *security* matters into

organization, screening, and licensing technologies (e.g. the NSABB). The third class of challenge remains under-addressed, as acknowledged by the NSABB.

During our engagement with SynBERC our calls to engage in exercises on the basis of the preceding analysis were not heeded. The aim of these *preparedness* exercises would be to build capacities for responding to events whose form, timing and impact cannot be known or calculated in advance.

The technique of scenario thinking entails a collective identification of goals and shared problems so as to orient future work. [1] The value of scenario thinking is its ability to "design and facilitate strategic conversations between key stakeholders that shift the focus from identifying constraints to imagining and pursuing shared opportunities. [It] facilitates dialogues that reveal and connect divergent perspectives into a more cohesive vision and commitment to action." [2] Scenarios provide a common framework and vocabulary for collaboration. If SynBERC were to engage in such work in the future, we propose that the organization adapt existing scenario techniques to identify blockages, norms, and practices that are tacit in their practice of synthetic biology and its emergent relations to the current security environment.

**Stage 1**

In stage 1, use scenario group processes and workshop design to create the collaborative framework within which we will be working during stages two and three. This collaborative framework can provide a common vocabulary and identification of critical uncertainties about the future of synthetic biology and keep application areas, such as biofuels.

Work should consist of three principal activities. First, interviews with SynBERC PIs, researchers from adjacent fields such a microbial ecology and other molecular sciences and actors with sufficient knowledge of the dynamics of global security milieus. This work would facilitate the agenda for scenario workshops. Second, conduct scenario workshops with specialists from aligned social science projects and scenario consulting group GBN. Third, collect critical uncertainties identified above and integrate them into working scenarios.

[1] Peter Schwartz (1998). *The Art of the Long View: Planning for the Future in an Uncertain World*. Wiley.

[2] www.gbn.com

**Stage 2**

In stage 2, facilitate collaborative working groups, using scenario frameworks developed in stage one. Design and conduct workshops for the dissemination and ongoing recursive refinement of these scenarios. These workshops would, if efficacious, provide insights for the ongoing adjustment of practices and institutions in synthetic biology.

Work in stage 2 would consist of three principal activities. First, facilitate ongoing collaborative working groups, adjusting and refining the processes used in these groups as work unfolds in synthetic biology and other salient domains. Second, conduct ongoing empirical research on developments in synthetic biology and developments in adjacent security and preparedness. The materials collected and analyzed from this research should be synthesized for use in the collaborative working groups and for working papers. Third, conduct dissemination workshops and host dissemination wikis for SynBERC researchers.

**Stage 3**

In stage 3, focus on applying insights developed in stages one and two. This would concentrate on the ways in which the evolving practices in synthetic biology suggest organizational and intuitional changes. It would also involve the development of a generalizable collaborative model for the production of responsible knowledge.

Bibliography

Alibek K (1999) *Biohazard* New York Random House
Allison , J (1988) *Power and Preparedness in Thucydides*, Baltimore MD, Johns Hopkins Press
Barr, M, (2008 ) Beyond Biosafety: Biosecurity and the dual-use dilemma as ethical concerns, *Eubios Journal of Asian and International Bioethics*, 18, 71-73
Beck , U (1995) *Ecological enlightenment : essays on the politics of the risk society*_Atlantic Highlands, N.J : Humanities Press,
Berg, P, Baltimore D, Brenner S, Roblin RO, and Singer MF, (1975) Asilomar conference on recombinant DNA molecules. *Science* 188: 991 – 994
Bugl et al (2007) DNA Synthesis and biological security, *Nature Biotechnology* 25, 627-629
Church G (2005) Let us go forth and safely multiply. *Nature* 438, 423
Collier, S and Lakoff A, (2008) Distributed Preparedness: Space, Security, and Citizenship in the United States. *Environment and Planning D: Space and Society* 26 (1) 7-28
Cook-Deegan et al.(2005) Issues in Biosecurity and Biosafety *Science Magazine* 24 June, 1867 – 1868
Dando, M (2006) *Bioterror and Biowarfare: A Beginner's Guide* Oxford Oneworld Publications
Douglas, M (1992) *Risk and blame : essays in cultural theory* London ; New York Routledge
Dröge M, Pühler A and Werner S (1998) Horizontal gene transfer as a biosafety issue: A natural phenomenon of public concern, *Journal of Biotechnology* 64, 75-90
Ewald, F (2002 ) The return of Descartes' malicious demon: An outline of a philosophy of precaution .In T.Baker and J Simon *Embracing risk: The changing culture of insurance and responsibility* Chicago, IL: University of Chicago
Fleming , Diane O Hunt , Debra Long (2006) *Biological Safety: Principles And Practices* ASM Press; 4 edition
Foucault, Michel (1976) *The will to knowledge: History of Sexuality: Volume1* London, Penguin
Foucault, Michel (2003) *Society Must be defended: Lectures at the College de France 1975-76* Picador
Foucault, Michel (2005) *The Hermeneutics of the Subject: Lectures at the College de France 1981-82* New York Palgrave Macmillan
Foucault, Michel (2007) *Security, territory, population : lectures at the Collège de France, 1977-78* New York Palgrave Macmillan
Garfinkel, M, Endy D ,Epstein G, Freidman R (2007) Synthetic Genomics: Options for Governance *Biosecurity and bioterrorism : biodefense strategy, practice, and science*. 4, 359-62.
Industry Association Synthetic Biology (2008) Workshop on Technical solution for Biosecurity http://www.ia-sb.eu/wp-content/uploads/2008/09/iasb_report_biosecurity_syntheticbiology.pdf accessed 6 December 2008
Kelle A (2007) Synthetic Biology & Biosecurity Awareness In Europe http://www.synbiosafe.eu/uploads///pdf/Synbiosafe-Biosecurity_awareness_in_Europe_Kelle.pdf accessed 6 December 2008
Kimman TG, E. Smit, and M. R. Klein (2008) Evidence-Based Biosafety: a Review of the Principles and Effectiveness of Microbiological Containment Measures. *Clin. Microbiol. Rev.* 21, 403-425
Lakoff, A(2008) The Generic Biothreat, or, how we became unprepared *Cultural Anthropology* 23( 3) 399-428
Lakoff, Andrew and Steven Collier (2008)*Biosecurity Interventions: Global Health and Security In Question* New York Columbia University Press
Laqueur, Walter (2003) *No End to War: Terrorism in the Twenty-First Century* New York Continuum
Luhmann, Niklas (1993) *Risk : a sociological theory* , New York A. de Gruyter,
Macintyre, Alisdair (1984) *After Virtue: a study in moral theory* Notre Dame University of Notre Dame Press
Maurer Stephen M , Keith V. Lucas & Starr Terrell (2006) From Understanding to Action: Community-Based Options for Improving Safety and Security in Synthetic Biology http://gspp.berkeley.edu/iths/UC%20White%20Paper.pdf accessed 6 December 2008
National Research Council (2004) Biotechnology Research in an Age of Terrorism National Academies Press http://www.nap.edu/catalog.php?record_id=10827 accessed 6 December 2008

National Science Advisory Board for Biosecuirty (2007) Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information, http://oba.od.nih.gov/biosecurity/pdf/Framework%20for%20transmittal%200807_Sept07.pdf accessed 6 December 2008

Nowotny, Helga Peter Scott, and Michael Gibbons (2001) *Re-Thinking Science: Knowledge and the Public in an Age of Uncertainty*. London Polity Press

O'Toole, Tara Thomas V. Inglesby (2003) Toward Biosecurity *Biosecurity and Bioterrorism*. 1(1): 1-3.

Rabinow, Paul (2007) *Marking Time: On the Anthropology of the Contemporary* , Princeton University Press

Rabinow, Paul and Gaymon Bennett (2008) *Ars Synthetica: Designs for Human Practice* [Connexions Web site] Available at: http://cnx.org/content/col10612/1.2/

Revill, James; Dando, Malcolm (2008 ) Life scientists and the need for a culture of responsibility: after education … what? *Science and Public Policy* 35, 29-35

Rheinberger, Hans-Jorg (1997) *Toward a History of Epistemic Things: Synthesizing Proteins in the Test Tube*, Stanford CA Stanford University Press

Segarra, Alejandro E. Fletcher Susan R. (2001)Biosafety Protocol for Genetically Modified Organisms, *Congressional Research Service - The Library of Congress*

Singer, M and Berg P (1976) Recombinant DNA: NIH Guidelines *Science* 193, 186-188

[1] This paper is a collaborative production of the Berkeley Human Practices Lab. Anthony Stavrianakis and Lyle Fearnley are communicating authors .

Stavrianakis at stavrianakis@berkeley.edu; Fearnley at lyle.fearnley@berkeley.edu)