Available online at www.sciencedirect.com
ScienceDirect
Research Policy 36 (2007) 1635–1654
research policy
www.elsevier.com/locate/respol

Biosecurity, bioterrorism and the governance of science: The increasing convergence of science and security policy

Caitríona McLeish [a,*], Paul Nightingale [b]

[a] SPRU, Freeman Centre, University of Sussex, BN1 9QE, UK
[b] CoPS Innovation Centre, SPRU, Freeman Centre, University of Sussex, BN1 9QE, UK

Received 17 March 2006; received in revised form 24 May 2007; accepted 4 October 2007

Abstract

Science and security policy are increasingly overlapping because of concerns that legitimate research might be misapplied to develop biological weapons. This has led to an expansion of security policy to cover broad areas of research and scientific practice, including funding, publishing, peer-review, employment, materials transfer, post-graduate teaching and academics' ability to design and perform experiments and disseminate research. Such changes raise policy concerns because many of the technologies used to produce biological weapons are 'dual use' and have legitimate peaceful applications. As a result, attempts to control their generation, diffusion or application can have unintended impacts on socially beneficial applications. This paper explores recent changes in the governance of science and technology and contributes to future policy making by assessing the relative merits of understanding the development of dual use policy in terms of either technology transfer or technology convergence.

Keywords: Biological weapons; Biosecurity; Bioterrorism; Biological weapons convention; Governance of science

1. Introduction

Perceptions within the security community that the threat from biological weapons is increasing, together with concerns that legitimate research might be misapplied and contribute to that threat, have led to an expansion of security policy to address areas of research that have traditionally been the domain of science policy. Biosecurity controls now influence scientific funding, peer-review, publication, employment, materials transfer, post-graduate teaching, international travel, and researchers' ability to construct, perform and disseminate research.[1] These measures are now so extensive that concerns have been raised about their impact on legitimate research (NRC, 2004; Enserink and Kaiser, 2005; IoM/NRC, 2006).

[1] All the changes discussed in the paper come under an overarching bio-security umbrella, but cover distinct areas: bio-terrorism (the threat or use of disease by non-state actors for political ends); bio-defence (the development of responses to biological warfare attack, including bioterrorism); dual-use controls (controls on technologies with legitimate and prohibited applications) and non-proliferation (controls on the diffusion of technologies to prevent their (illegal) hostile use).

* Corresponding author. Tel.: +44 1273 873556; fax: +44 1273 685865.
E-mail addresses: c.a.mcleish@sussex.ac.uk (C. McLeish), p.nightingale@sussex.ac.uk (P. Nightingale).

0048-7333/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.respol.2007.10.003

This paper aims to contribute towards the practical development of improved biosecurity policy by exploring the merits of different ways of understanding biosecurity controls and their role in preventing the proliferation of technological capabilities related to the development and production of biological weapons as defined in the 1972 *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction* (BWC). A particular concern within the paper is 'dual use' which refers to the tangible and intangible features of technologies that enable them to be applied to both (illegal) hostile and peaceful ends with little or no modification (Molas-Gallart and Robinson, 1997). As such, the term is used to highlight how the same upstream activities, materials, information and equipment can potentially have both (illegal) hostile and peaceful downstream applications.

When the term 'dual use' first entered the technology policy literature, it had positive connotations related to the benefits generated by reusing civilian technologies to develop military technologies (Alic et al., 1992; Alic, 1993; Cowan and Foray, 1995; Reppy, 1999; Molas-Gallart, 1997, 2000, 2002; on technology transfer see Bozeman, 2000). Since the late 1970s, however, 'dual use' has taken on significantly more negative connotations and now applies to the potential of technologies with legitimate civilian uses to aid the proliferation of prohibited military technologies (Roberts, 1995; United Nations General Assembly, 1977; see Molas-Gallart, 1996, p. 6). In particular, it is applied to technologies with legitimate application in scientific research, drug/vaccine production, agriculture or industrial processing that could be misappropriated to produce chemical or biological weapons (McLeish, 2002).

Although dual use (in its second, negative sense) has been recognised since the 17th century (Bacon, 1609) and the term has been used within the arms control and disarmament communities since the 1940s (and the establishment of CoCom (Coordinating Committee for Multilateral Export Controls) (Reppy, 2006), the science policy issues it generates have only become fully appreciated as the threat posed by biological weapons, and their links to the life sciences, has grown. These concerns achieved widespread public prominence following the publication of three papers – one on the synthesis of polio virus cDNA without a natural template by Cello et al. (2002); another on how the variola virus (smallpox) can evade the immune system by Rosengard et al. (2002); and a third on overcoming resistance to mouse-pox by Jackson et al. (2001) – that were widely interpreted as "publishing a blueprint" for terrorists and led to public calls for changes to research and publication procedures (Wallerstein, 2002; Cozzavelli, 2003; Malakoff, 2003; Purver, 2002; Danchin, 2002; Finkel, 2001; Kahn, 2004).[2]

Such changes are part of an escalation of biological weapons policy following the failure of the international negotiations to strengthen the BWC in July 2001 and the posting of letters containing the causative agent of Anthrax in the US in the Autumn of 2001.[3] Since then, the close historical relationship between the life sciences and biological weapons development (Guillemin, 2005; Balmer, 2002, 2001, 1997; Fraser and Dando, 2001; Leitenberg, 2001) has been recast as a significant policy issue (Martin, 2002) with discussions of threat-levels suggesting that advances in the life sciences and the spread of legitimate biotechnology are increasing the number of actors who could access biological warfare (BW) technologies. As a result, a range of policy measures have been initiated (Lentzos, 2006; NRC, 2004; Gaudioso and Salerno, 2004; Atlas, 2002) and funding for biosecurity research has significantly increased (up 3200% since 2001 at the National Institutes of Health (Harris and Steinbruner, 2005, p. 1)).[4]

Dual use complicates the design and implementation of these new policies because they must address the diffusion of socially beneficial technologies that are often controlled by non-state actors outside the traditional remit of security policy. Policies that disrupt the acquisition and exploitation of dual use technologies therefore have the potential to generate substantial social costs (McLeish and Nightingale, 2005; NRC, 2004; Gaudioso and Salerno, 2004; Altman et al., 2005; Atlas, 2001, 2002; Robinson, 1997; NAS, 1982; Breithaupt, 2000). Both the security and scientific policy communities therefore face a dilemma: how to design policies that can simultaneously successfully suppress biological weapons development whilst accommodating and

[2] See for example, Representative Dave Weldon's House Resolution 514 in response to the polio synthesis paper (26 July 2002 House of Representatives, 107th Congress). However, the method had been available since 1981, was laborious, and was interesting because of *weakened* pathogenicity (NRC, 2004, p. 22).

[3] Other factors include the discovery of the extent of the USSR and Iraqi biological weapons programs and how much both drew on dual use facilities; rapid advances in relevant biological sciences (vaccinology, immunology, pathogenesis and zoonosis); and the international diffusion of technical capabilities through dual use technologies.

[4] For example, many journals require authors to provide research materials on request as a condition of publication, which might now be subject to national and international legal restraints (Danchin, 2002; Breithaupt, 2000; Musser, 2001).

even encouraging the spread of dual use technologies for legitimate technical and scientific reasons?

This paper aims to address this dual use dilemma and assist policymaking in two areas. First, in relation to science policy, the paper draws on the security and the governance literature (Müller, 1995; Krasner, 1983; and Braithwaite and Drahos, 2000) to show how seemingly unrelated internal changes in the science system are part of a coherent expansion of an external security regime. Secondly, in relation to security policy the paper draws on the science policy literature (Rosenberg, 1963; Nightingale, 2004) to evaluate the advantages and disadvantages of understanding governance of dual use in terms of either technology transfer or technology convergence.

The paper is divided into a further three sections. Section 2 explores how recent policy measures that govern research fit into a wider set of changes within the anti-BW regime. Section 3 addresses the main concern of this paper: how these changes should be understood. It examines how understanding the dual use problem in its current terms (i.e. as a technology transfer problem) generates policies directed at artefacts that aim to prevent the transfers of dangerous technologies from science. An alternative framework, which understands the dual use problem in terms of technological convergence, is then presented that directs policies at purposes, and aims to disrupt innovation processes. This (1) permits a more subtle analysis of the complex interactions between scientific research and technological development, (2) highlights important differences between (so called) 'dangerous' science, weapons and weapons of mass destruction, and (3) by emphasising purposes not things, helps prevent policies being overtaken by changes in science and technology. Section 4 addresses policy implications.

2. The biological weapons problem

Biological weapons are prohibited by rules of customary and treaty-based international law that embody ancient norms against the hostile use of disease. They therefore do not present a traditional, state-centric 'disarmament' or 'arms control' security problem because they are already banned and should not exist. Instead the policy problem they raise involves maintaining respect for existing prohibitions and addressing weaknesses in the protective regime resulting from the emergence of new threats.[5]

As an international security policy issue, the problem posed by biological weapons became more prominent after threats to international security were redefined at the end of the Cold War. In 1992, the summit session of the United Nations Security Council highlighted weapons of mass destruction as the greatest threat to international peace and outlined a course of action involving "the members of the Council comit[ing] themselves to working to *prevent the spread of technology* related to the *research for* or production of such weapons and to take appropriate action to that end" (emphasis added, UNSC, 1992). This reflected both a changing security threat and the perception that advances in science and technology (in particular advances in 'microbiology, biotechnology, molecular biology, genetic engineering, and any applications resulting from genome studies' (Fourth Review, 1996) were opening up new opportunities for weapons development.[6]

These concerns focused international policy attention on the weaknesses of the existing regime for governing biological weapons and in 1995 negotiations began to reinforce the BWC through an additional legally binding instrument – the BWC Protocol. However, for a variety of reasons, negotiations collapsed in 2001 (Littlewood, 2005) and a new 'intersessional process' of annual talks was introduced. It is in the context of this change in perceptions of (a) threat, (b) scientific opportunity and (c) the potential of traditional multilateral governance measures to address those threats that new

[5] As Littlewood notes, the biological weapons policy problem: "has no connection to the problems under the [Nuclear Non Proliferation Treaty] related to discrimination between different categories of states; it is not about ... disarmament because no state under the BWC is permitted to have biological weapons; it has no connection to oversight of destruction of ... chemical weapons within six states (Albania, India, Libya, Republic of Korea, Russia, US) under the 1993 Chemical Weapons Convention" (2004, p. 3).

[6] At the next Review Conference, the UK delegation highlighted the '*great advance in a number of fields which provide understanding of the genetic, structural and functional basis of micro-organisms and toxins, and in the number and sophistication of techniques able to make directed changes to the properties of micro-organisms or toxins*.' (UK 2001). The UK review contained detailed sections on genomics and proteomics; bioinformatics; gene therapy; virulence and pathogenicity; vaccines and novel therapies; recombinant protein expression; toxins and other bioactive molecules; drug resistance; disease and pest control in agriculture; molecular biology applications and crops; and protein production technologies (ibid). Similarly, the American delegation highlighted '*major advances have occurred in ... genetic modification, genomics, proteomics, bioremediation, bio-control agents, vaccine development and bioinformatics [and] of special interest to the BWC are applications in directed molecular evolution*' (USA, 2001). They went on to note their dual use potential: "*While offering obvious benefits to mankind, advances in technology can be used to produce new substances or modify old ones and lead to novel and significant toxins and biological and biochemical weapons threats*.' (ibid).

governance measures that address research have been introduced.[7]

2.1. Multilateral controls

The new measures reinforce an existing regime that is 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 – intended to prevent the spread of dangerous weapons and technologies. The normative backbone of the regime (Hasenclever et al., 1997) is the 1972 *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction* (BWC) which sets out, and clearly establishes, through a framework of rules and norms, a sense of what is and what is not legitimate behaviour. The treaty currently has 159 states parties and 15 signatories.[8] Under the Convention State parties are "determined, for the sake of all mankind, to exclude completely the possibility of bacteriological (biological) agents and toxins being used as weapons" to which end they obligate themselves:

> never in any circumstances to develop, produce, stockpile, or otherwise acquire or retain:
>
> 1. Microbial or other biological agents or toxins whatever their origin or method of production of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes.
> 2. Weapons equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict [emphasis added].

The treaty consequently covers all phases of the armament process except research,[9] with members also obligating themselves not to provide assistance to any state, group of states or international organisations. This article also recognises, in the words underlined, the dual use problem. Known as the General Purpose Criterion these underlined words define the scope of the treaty by prohibiting all purposes other than "peaceful purposes". Because the Treaty bans purposes rather than 'things' its prohibitions cannot be innovated around, and it embodies the norm in a timeless form.[10]

The rules and obligations of the BWC are operationalised through national laws and regulations. In order to prevent individuals from performing actions it prohibits to states, the BWC requires its parties to

> take any necessary measures to prohibit and prevent the development, production, stockpiling, acquisition or retention of the agents, toxins, weapons, equipment and means of delivery specified in Article I of the Convention, within the territory of such state, under its jurisdiction or under its control anywhere (Article 4).

In the United Kingdom the BWC was implemented in *The Biological Weapons Act* (1974) which makes it a criminal offence to develop, produce, stockpile, acquire or retain any biological agent, toxin or means of delivery that has no justification for peaceful purposes.[11] Similarly, when the BWC was implemented in the USA through the *Biological Weapons Act* (1989) it became a criminal offence, with extraterritorial federal jurisdiction when committed by or against a US national, to produce, develop, transfer, acquire, retain, or possess any "biological agent, toxin, or delivery system for use as a weapon" or provide aid to anyone doing so.[12] In both instances, the overarching national prohibitions cover purposes prohibited by the BWC.

[7] These measures include a shift towards implementing bio-safety guidelines, regulating access to pathogens, reporting disease outbreaks and developing ethical codes of conduct.

[8] As of 1 November 2007.

[9] While the BWC does not directly address use, the 1925 *Protocol for the prohibition of the use in war of asphyxiating, poisonous or other gases, and of bacteriological methods of warfare* (The Geneva Protocol) prohibits use and is widely accepted to have achieved the status of customary international law (Greenwood, 2000, pp. 802–805). This was reaffirmed in the final document of the BWC's Fourth Review Conference in 1996 (Fourth Review, 1996).

[10] Changes in technology can cause the letter of the law to diverge from the spirit of the law. The 1923 *Hague Draft Rules on Aerial Warfare*, for example, defined legitimate military targets using lists that were constantly made out of date by changing technology. As a result, an approach that addresses purposes rather than things was introduced. Additional Protocol I, Article 52(2) now limits military objectives to 'those objects which by their nature, location, purpose or use make an effective contribution to military action and those total or partial destruction, capture or neutralisation ... offers a definite military advantage.' (Greenwood, 2000, p. 797).

[11] These prohibitions were extended to cover the transfer of materials under the *Anti Terrorism Crime and Security Act* (2001) which also extended jurisdiction beyond the UK to acts committed by UK nationals.

[12] This offence was extended by the *Antiterrorism and Effective Death Penalty Act* (1996) which criminalized the threat to use biological weapons.

2.2. Additional policy measures—export controls and PSI

Although the BWC covers the full spectrum of risk from states, terrorists or criminals, there is "no one size fits all" policy solution (Littlewood, 2004, 2005; Chyba and Greninger, 2004) and additional policy measures have been introduced to govern weapons-related technologies. Since many of these technologies are dual use they cannot be easily banned. States have therefore used export controls to suppress the hostile application of dual use technologies while promoting their diffusion for legitimate purposes.[13] By understanding the security problem in terms of technology transfer, export controls rely on judgements about the intent of the requesting party to ensure that technology is only transferred to recipients that are not regarded as a cause for concern (Defense Science Board, 2000). The Australia Group, for example, was set up in 1984/1985 in response to evidence that Iraq had sourced precursor chemicals and materials for its chemical warfare program through legitimate channels (Robinson, 1992; Zilinskas, 1999). It aims to "*limit the risks of proliferation and terrorism involving chemical and biological weapons by controlling transfers of technology that could contribute to chemical and/or biological weapons activities by states or non-state actors*".[14] This is done through harmonized licensing measures that cover exports of technology on the Group's common control lists.[15]

Similarly, the 1993 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies covers conventional weapons, WMD and delivery systems and promotes transparency and the exchange of information on transfers of conventional arms and dual-use technologies.[16] For tangible technology transfers, the participating states agree a regularly updated list of controlled technologies[17] "*which are major or key elements for the indigenous development, production, use or enhancement of military capabilities*".[18] In 2000, the controls were extended to intangible technology transfers that emphasized both intangible technology (software) and intangible transfer such as face to face discussion, fax, email or telephone conversations.[19] Technology is defined within the arrangement as "*Specific information necessary for the 'development', 'production' or 'use' of a product. The information takes the form of technical data or technical assistance*" and therefore covers areas of research and development.[20]

The rise of the "proliferation-terrorism nexus" (Ellis, 2003) has led to recognition that while export control measures help prevent flows of technology from member states with high levels of endogenous technology to countries of concern (with lower levels of technological capabilities), they are insufficient to prevent the diffusion of technology from states that are not party to the various export control regimes and agreements. This channel of technology transfer has caused states to implement measures which address the approximately 21 states that are not yet signatories of

[13] Export controls existed before the Cold War. For example, in the UK *The Import, Export and Customs Powers (Defence) Act* was passed in 1939 to control UK imports and exports. A short amending Act, the *Import and Export Control Act*, 1990, removed a section of the 1939 Act, which provided for expiry on the making of an Order declaring the 'emergency' to be over.

[14] http://www.australiagroup.net/en/guidelines.html.

[15] While these lists are updated to take account of changes in technology they also include a 'catch-all clause' directed at purposes. The lists include chemicals, biological agents, pathogens and certain chemical and biological equipment. See http://www.australiagroup.net/en/agact.htm. The lists are comprehensive—the biological equipment list covers common technologies such as fermentors, centrifugal separators, freeze drying equipment and aerosol inhalation chambers; while the biological agent list currently includes 32 viruses; 4 rickettsiae; 15 bacteria and 19 toxins and subunits thereof, as well as genetic elements and genetically modified organisms associated with these agents (except in the form of a vaccine). The controls do not apply to information 'in the public domain', 'basic scientific research' or for patent application. http://www.australiagroup.net/en/control_list/bio_agents.htm.

[16] The arrangement is open on a global and non-discriminatory basis to prospective states that are producers/exporters of arms or industrial equipment; maintain appropriate non-proliferation policies, including adherence to relevant non-proliferation regimes and treaties and effective export controls.

[17] http://www.wassenaar.org/list/wa-listTableOfContents.htm.

[18] Wassenaar Agreement. *Criteria for the selection of dual-use items*, as agreed December 2004 See Wassenaar Agreement. Criteria for the selection of dual-use items, as agreed December 2004 See http://www.wassenaar.org/list/Criteria%20for%20DU%20List%20including%20SL%20and%20VSL%20for%20WEb%20Site.doc.

[19] Similarly, the *Export Control Act* (2002) and *Export of Goods, Transfer of Technology and Provision of Technical Assistance (Control) Order* (2003) define 'technology' as including '*information (including but not limited to information comprised in software and documents such as blueprints, manuals, diagrams and designs) that is capable of use in connection with the development, production or use of any (prohibited) goods*'.

[20] 'Technical data' could be blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and *instructions*. While 'technical assistance' can involve instruction, skills, training, working knowledge and consulting services (ibid). See http://www.wassenaar.org/controllists/16%20-%20WA-LIST%20%2804%29%202%20-%20DEF.doc; http://www.wassenaar.org/publicdocuments/Basic%20documents%202005%20-%20September.doc.

the BWC (and are therefore not yet obliged to implement the BWC prohibitions at the national level). The Proliferation Security Initiative (PSI), for example, was launched in 2004, with the support of over 60 countries, to counter the development of WMD by non-state actors (such as terrorists) and states of concern (Byers, 2004; Joyner, 2004) and involves the interception of shipments of sensitive materials, equipment and technology, typically at sea, from proliferating states. Similarly, UN Security Council Resolution 1540 (2004) obligates all UN member states to refrain from providing any support to non-state actors attempting to acquire, use or transfer WMD and their delivery systems. It states that in accordance with 'their national procedures [states], shall adopt and enforce appropriate effective laws which prohibit any non-state actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes' (see UN, 2004; Oosthuizen and Wilmshurst, 2004; Kellman, 2004).

This focus on non-state actors marks a new development in biosecurity policy, which historically has been state-centric because only states were able to afford to development biological weapons (Koblentz, 2003; Guillemin, 2004). The increased perception of threat from bioterrorists (Noble, 2006; Cameron, 1999) and the diffusion of dual-use biological technologies has meant that non-state actors are now seen as both sources of threat and as sources of technological capabilities. As a result, the regime has evolved and governments are now enrolling actors not normally associated with security by introducing new controls on people, experiments and the flow of information, technology and materials. These national controls are now the main vehicles that govern scientific activity (Kellman, 2001).

2.3. National transfer and access measures

New biosecurity controls now cover the transfer of specific biological agents within and across national boarders. In the US this is done through 'select agent' controls.[21] *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act*, 2001, requires that no 'restricted person' shall possess, transport or receive select agents.[22] While, the *Public Health Security and Bioterrorism Preparedness and Response Act*, 2002 requires that all individuals wishing to have access to, possess, use, work with or transfer select agents undergo registration to ensure that they are not 'restricted persons'.[23] This involves a security assessment (including fingerprinting) conducted by the FBI, followed by approval by either the Centres for Disease Control and Prevention (CDC) or the US Department of Agriculture's Animal and Plant Health Inspection Service (APHIS).[24]

The UK has a similar list in Schedule 5 of the *Anti Terrorism Crime and Security Act* (2001) which obliges the occupier of any premises to notify the Secretary of State before any dangerous substance is kept or used there.[25] If required to, the occupier must release this information to a senior police officer together with a list of people who have access to the premises or any dangerous substance.[26] If there are reasonable grounds for believing that security measures are inadequate, the Secretary of State can require the occupier to dispose of

[21] 'Select agents' are defined as "biological agents or toxins deemed a threat to the public, animal or plant health, or to animal or plant products", and currently involve 33 viruses; 1 prion; 11 toxins; 19 bacterium and 6 fungi. Also covered are genetic elements, recombinant nucleic acids and recombinant organisms associated with the select agents as well as experiments which involve either the deliberate transfer of a drug resistance trait to a listed agents or the deliberate formation of rDNA for the biosynthesis of certain listed toxins. (As of November 2005).

[22] 'Restricted persons' are defined as an individual who: Is under indictment [or has been convicted] for a crime punishable by imprisonment for a term exceeding 1 year; ... Is a fugitive from justice; Is an unlawful user of any controlled substance; Is an alien illegally or unlawfully in the United States; Has been adjudicated as a mental defective or has been committed to any mental institution; Is an alien [without permanent residence] ... who is a national of a country [that] ... the Secretary of State... has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism; or Has been discharged from the Armed Services of the United States under dishonorable conditions. Sec. 817. Expansion Of The Biological Weapons Statute, *Uniting and Strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act*, 2001 Public Law 107–56.

[23] Paragraph b: Regulation of Transfers of Listed Agents and Toxins, Section 351A. Enhanced Control of Dangerous Biological Agents and Toxins, *Public Health Security and Bioterrorism Preparedness and Response Act*, 2002.

[24] The assessment is valid for three years and is subject to CDC or APHIS termination. The act requires the Secretary of Health and Human Services to maintain a database of such individuals and the select agents they can access.

[25] Currently the list contains 19 viruses, 5 rickettsiae, 13 bacteria, 11 toxins and covers their genetic material or genetically modified organisms containing a sequence of a listed agent. Paragraph 59 "Duty to notify Secretary of State before keeping or using dangerous substances", Part 7 Security of Pathogens and Toxins, *Anti Terrorism Crime and Security Act*, 2001.

[26] Paragraph 61 "Information about persons with access to dangerous substances" Part 7 Security of Pathogens and Toxins, *Anti Terrorism Crime and Security Act*, 2001.

the substance and can also prevent an individual from having access to dangerous materials and/or parts of the premises.[27] For an assessment see McLeish (2004).

2.4. Other governance measures covering scientists

The potential for student training to be used to diffuse technological capabilities is well recognised by the security community and vetting schemes for students operate in both the UK and the USA.[28] The UK scheme, which began in 1994, was developed after it became apparent that a number of State proliferators had exploited UK trained scientists.[29] The scheme is administered by the Foreign and Commonwealth Office (FCO) and covers post-graduate students and post-doctoral researchers from 10 countries working in 21 academic disciplines of concern that are relevant to the development of WMD or their delivery systems.[30] Under the scheme higher education institutions can voluntarily seek government advice about whether an application should be regarded as a proliferation risk. According to information released under the *Freedom of Information Act* (2005) the numbers of referrals has grown from 4 in 1998 to 740 in 2002.[31]

Similar programs exist in the USA. Section 416 of the *Patriot Act* required the Attorney General to implement the foreign student visa-monitoring program established by the *Illegal Immigration Reform and Immigrant Responsibility Act* (1996) by 1 January 2003, and expands the program to include educational institutions such as flight, language training, and vocational schools. While, Section 501 of the *Enhanced Border Security and Visa Entry Reform Act*, 2002 establishes a Foreign Student Monitoring Program to maintain up-to-date information on foreign students and exchange visitors.

Science and engineering disciplines are disproportionately affected by these measures because visa applicants are more likely to study subjects on the US Government's Technology Alert List. As a result, they incur greater security checks by the (US) Visas Mantis Program—the multi-agency, security review that identifies visa applicants who may pose a threat to national security.[32] Since 2001 surveys have indicated visa controls are reducing the number of foreign students enrolling in the US (Arnone, 2004; Council of Graduate Schools, 2004) and the Presidents of the US National Academies of Sciences have suggested they are damaging US science.[33] In 2005, 40 leading scientific societies and higher education associations released a joint statement calling for modifications to restrictions on foreign researchers because the US "risk[s] irreparable damage to our competitive advantage in attracting international students, scholars, scientists, and engineers, and ultimately to our nation's global leadership".[34]

[27] Paragraph 63 "Directions requiring disposal of dangerous substances" and Paragraph 64 "Directions requiring denial of access" Part 7 Security of Pathogens and Toxins, *Anti Terrorism Crime and Security Act*, 2001.

[28] For example, the Corson report (NAS, 1982, p. 15), highlighted scientific and technical apprenticeships as the leading knowledge diffusion concern of the US intelligence community.

[29] The UK FCO convened an 'awareness raising seminar' on 10 March 1993 to explain new export controls and launch a BW booklet, during which the government floated the idea of vetting overseas students (Wilkie, 1993, p. 1.) A year later the voluntary vetting scheme (VVS) was launched to "stop individuals from certain countries which we [FCO] regard as proliferators or potential proliferators of WMD from taking courses which would help them acquire *the knowledge necessary to assist with the production or manufacture (proliferation) of WMD* within their home country and which might one day threaten the UK's national security" (emphasis added <www.fco.gov.uk/Files/kfile/VVS.doc>). For more on VVS see 'Dr. Howells for the Secretary of State for Education and Employment to Mr. Brake' *Hansard (Commons)*, written answers, vol. 307, 25 February 1997, col. 295, <http://www.publications.parliament.uk/pa/cm200203/cmselect/cmsctech/415/415ap56.htm>. See also 'Mr Boswell for the Secretary of State for Education to Mr Willetts' *Hansard (Commons)*, written answers, vol. 247, 19 July 1994, col. 137–138.

[30] Countries covered include Cuba, India, Egypt, Iran, Iraq, Libya, Israel, North Korea, Pakistan and Syria. The subjects include chemistry, biology, physics (including nuclear), mathematics, computing science and mechanical, chemical and control engineering.

[31] See http://www.fco.gov.uk/Files/kfile/VVS.doc. For suggested problems see the evidence submitted on 14 May 2003 by the Association of Heads of Universities to the House of Commons Select Committee on Science and Technology available at http://www.publications.parliament.uk/pa/cm200203/cmselect/cmsctech/415/415ap56.htm At the time of writing plans have been announced by the UK government to relaunch the scheme as a compulsory measure affecting the applications of any post-graduate student from outside the EU coming to UK universities to study scientific disciplines that are considered relevant to the development of WMD or their delivery systems (Gilbert, 2007).

[32] http://www.aaas.org/spp/post911/visas/.

[33] See Recommendations for Enhancing the US Visa System to Advance America's Scientific and Economic Competitiveness and National Security Interests (13 December 2002). http://www4.nationalacademies.org/news.nsf/isbn/s12132002?OpenDocument. Section 5301 of the *Intelligence Reform and Terrorism Prevention Act*, 2004 added a new section (222(h)) to the Immigration and Nationality Act (as amended 1996) which sets out statutory requirements for personal interviews of non-immigrant visa applicants.

[34] Available at Available at http://www7.nationalacademies.org/visas/May%2018%20Joint%20Statement.pdf.

2.5. Governance measures covering scientific information and experiments

Biosecurity concerns have also led to changes in scientists' freedom to disseminate results. In the United States the traditional balance between national security and freedom to publish was established in National Security Decision Directive 189 which guaranteed that there would be "no restrictions ... upon the conduct or reporting of federally funded fundamental research that has not received national security classification" (USA, 1985).[35] The directive was issued by former President Ronald Reagan in 1985 and reaffirmed by National Security Advisor Condoleezza Rice in November 2001. Shortly afterwards the term 'sensitive but unclassified' was introduced to preserve confidentiality without formal classification, and in January 2002 more than 6500 declassified documents relating to sensitive chemical and biological warfare information began to be withdrawn from public access.[36]

Because not all dual use research is under government control, self-governance measures to control the dissemination of information have also been introduced by the US scientific community.[37] Following a White House proposal that journal editors not publish "sections of articles that give experimental details researchers ... would need to replicate the claimed results" and create biological weapons (Broad, 2002), the American Society for Microbiology (ASM) which publishes Infection and Immunity, Journal of Bacteriology and Journal of Virology, adopted new publication guidelines in August 2002. These require reviewers to inform editors of manuscripts containing information which "might be misused or might pose a threat to public health [sic] safety" (Atlas, 2002).[38] The impact of these new prepublication controls has been relatively light: of the 13,929 manuscripts submitted to ASM journals in 2002, 313 'select agent' manuscripts received special screening and only two received additional screening by the full ASM publication board (NRC, 2004, p. 83).

Similarly, following the calls for changes to the Mertonian norms (Merton, 1973) and publication procedures that promote widespread diffusion of scientific information noted in the introduction, 34 journal editors, including the editors of *Science*, *Cell* and *Nature*, issued preliminary suggestions for a self-governing framework for peer-review. In a commentary published in *Nature* the editors stated:

> Scientists and their journals should consider the appropriate level and design of processes to accomplish effective review of papers that raise such security issues ... We recognise that on occasion an editor may conclude that the potential harm of publication outweighs the potential societal benefits. Under such circumstances the paper should be modified or not published.[39]

Such concerns led the National Research Council of the US National Academies to convene an expert panel under the chairmanship of Professor Gerald Fink to address the science policy issues raised by dual use research (Harris and Steinbruner, 2005). While the resulting report – *Biotechnology research in an age of terrorism: confronting the dual use dilemma* (2004) – recognised that other dissemination routes exist,[40] it recommended pre-publication reviews of manuscripts with particular scrutiny for publications about experiments that:

1. Would demonstrate how to render a vaccine ineffective.
2. Would confer resistance to therapeutically useful antibiotics or antiviral agents.
3. Would enhance the virulence of a pathogen or render a non-pathogen virulent.
4. Would increase transmissibility of a pathogen.
5. Would alter the host range of a pathogen.

[35] Available at Available at www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

[36] http://www.aaas.org/spp/post911/sbu/. See NAS (1982) for similar Cold War measures.

[37] Similar controls were introduced to cover nuclear research in the early 1940s when the joint National Academy of Sciences-National Research Council "Advisory Committee on Scientific Publications" headed by Luther P. Eisenhart explored restricting publication of sensitive information and secured the co-operation of 237 scientific journals (Cochrane, 1978, pp. 386–387). These issues were also addressed in the context of the diffusion of scientific knowledge related to nuclear technology to the Soviet Union by the Corson Report (NAS, 1982).

[38] Testimony of Dr. Ron Atlas of the American Society for Microbiology before the House of Representatives Committee on Science 10 October 2002, available at Testimony of Dr. Ron Atlas of the American Society for Microbiology before the House of Representatives Committee on Science 10 October 2002, available at http://www.house.gov/science/hearings/full02/oct10/atlas.htm.

[39] They justified their action by stating: 'We recognise that the prospect of bioterrorism has raised legitimate concerns about the potential abuse of published information ... we are committed to dealing responsibly and effectively with safety and security issues that may be raised by papers submitted for publication, and to increasing our capacity to identify such issues as they arise' (Nature Editorial, 2003).

[40] For example, presentations at scientific meetings, Internet postings, email exchanges.

6. Would enable the evasion of diagnostic detection modalities; or
7. Would enable the weaponisation of a biological agent or toxin (NRC, 2004).

The Fink Report was followed by an *ad hoc* committee of the National Research Council and the Institute of Medicine – Committee on Advances in Technology and the Prevention of their Application to Next General Biowarfare Threats – which examined how life sciences and other disciplines (e.g. nanotechnology), might enable the development of new generations of biological threats over the next 5–10 years (IoM and NRC, 2006). The committee made recommendations for a 'broad-based intertwined network of steps . . . for reducing the likelihood that [relevant] technologies . . . will be used successfully for malevolent purposes' (ibid, p. 4). The committee endorsed policies that to 'the maximum extent possible, promote the free and open exchange of information in the life sciences' and recommended adopting a broader perspective on the 'threat spectrum' to recognise the inherent limitations of agent-specific threat lists. It also recommended strengthening the technical expertise of the security communities; the promotion of a common culture of awareness and responsibility within the global life science community; and that public health infrastructure and response and recovery capabilities be strengthened (ibid, p. 5).

3. Designing effective policy: the importance of framing assumptions

These new governance measures have drawn heavily on measures previously used for nuclear and chemical weapons. While modelling policies in one area on successful policies in other related areas is a standard part of technology governance (Braithwaite, 1994; Braithwaite and Drahos, 2000), its success is dependent on the appropriateness of the extrapolation, which, in turn, depends on the appropriateness of the implicit (framing) assumptions (Acha, 2002) that are used.

The fact that biological weapons are biological, for example, is likely to influence the success of the extrapolation. For example, pathogens can be grown with readily available feed-stocks, which makes the materials-balance verification methods used for organophosphates and enriched uranium problematic to apply. Additionally, pathogens can be grown rapidly, suggesting it might be possible to scale up production faster than nuclear and (to a lesser extent) chemical weapons. And finally, the underlying science and technologies behind biology are rapidly advancing and diffusing globally, so that the capabilities required to develop advanced weapons are perceived to be becoming easier to acquire.

Secondly, policy making is simpler when technologies have a single military use as it is often possible to hinder access to weapons by controlling access to artefacts, even if, as was the case with the Soviet nuclear program, it is possible to eventually innovate around controls. With biological weapons, however, states have legitimate reasons for acquiring and developing dual use technologies. As a result, controls can generate greater social costs; technologies tend to be more widely diffused; and their diffusion in organisations such as universities and firms increases the number of actors of security concern who can have entirely legitimate concerns about the impact of controls. Dual use technologies also allow states to develop their own indigenous biotechnology capabilities more easily than with nuclear technologies, suggesting that the effectiveness of measures like export controls or vetting schemes, that rely on imbalances between states' indigenous technological capability, might become limited in the future.

Thirdly, the definitions, models and understandings of technology that are used by both analysts and actors have changed substantially since many of governance measures for nuclear technologies were developed. During the early Cold War period understanding focused on physical artefacts, then technology was understood in terms of bodies of knowledge reflecting the *techne* and *-ology* of technology (Pavitt, 1999; Rosenberg, 1982; Freeman, 1982). Today, technology is understood in terms of both artefacts (tangible and intangible) *and* socially distributed bodies of knowledge, both of which only generate functions through interactions with a wider technological infrastructure or regime (Nightingale, 2004). Similar changes have occurred in understanding of the relationship between science and technology. In the 1950s and 1960s the focus was on linear models (both science push and market pull), then understanding moved towards 'coupling models' that linked research with market demands (Rothwell, 1977; Kline and Rosenberg, 1986) and then towards systems models that take into account institutions that promote the accumulation and diffusion of technological capabilities (Martin and Nightingale, 2000). Within these later models, science is far less likely to take centre stage; there is much more appreciation of sectoral variety (Pavitt, 1984; Archibugi, 2001); and how the indirect relationships between science and technology (Rosenberg, 1982) is influenced by tacit, person-embodied problem solving skills, instrumentation and access to networks (rather

than the simple diffusion of information in scientific papers) (Gibbons and Johnston, 1974; Hicks, 1995).

And finally, when extrapolating from one successful regime to another, it is not always clear what should be extrapolated. For example, the success of the nuclear regime could be the clear focus on preventing the diversion of civilian fissile material to military applications. Or, it could be that the Three Mile Island accident created a 'community of shared fate' within the nuclear industry, which was reinforced by the international insurance industry, to drive security and safety standards upwards (Braithwaite and Drahos, 2000). Or, it could be because a flexible approach was put in place that could adapt to unpredictable changes. Or, it could be that the regime has developed an almost perfect 'enforcement pyramid' (Braithwaite, 1993, 2002) with a clearly defined path of increasingly coercive measures, from informal cooperative discussion directly up to the UN Security Council. As this example shows, directly extrapolating from one regime to another is often dependent on (implicit) assumptions about success factors.

These variations in framing assumptions can have a major influence on policy formulation. For example, an extreme linear model of technical change, that only focused on prohibited uses and directly extrapolated from measures that worked for nuclear technologies might generate polices that focus on restricting the diffusion of dangerous scientific information, pathogens and materials. However, linear models under-estimate the costs of development compared to research (and therefore the technical difficulties involved in developing biological weapons), overlook the non-scientific knowledge that has to be integrated to develop technology, and focus inappropriately on high-tech research (cf., Rosenberg, 1982; Pavitt, 1999). Furthermore, by solely focusing on hostile applications, such models overlook the socially beneficial outputs of research. As a result, policies are likely to over-estimate the benefits of controls, under-estimate their costs, overlook alternatives and be ineffective.

While some of the initial reactions to the publications of the papers listed in the introduction came close to this model, within the main policy discourse the traditional way of thinking about dual use policy remains in terms of technology transfer. The next section critically evaluates this model and compares it to an alternative model where dual use is understood in terms of technological convergence. These differences suggest that while it is useful to extrapolate from successful experiences in other policy environments, it may not necessarily be the best solution.

3.1. Understanding dual use

The differences between the two models of dual use considered here relate to how they conceptualise the relationship between an artefact and its technological function. The traditional way of understanding technology regards technological functions as intrinsic, and innovation as primarily about an (Schumpeterian) inventive *event* that creates a technology with a fixed function that is then diffused in a relatively costless fashion. Consequently, the traditional way of understanding dual use technologies sees them as having intrinsic (fixed) functions which can be applied in both civilian and (prohibited) military settings. Since the technological function is dangerous then so is the dual use science or technology that is transferred. The policy problem is therefore understood in terms of *technology transfer* and preventing *intrinsically* dangerous research and technology getting into hostile hands.

An alternative framing of dual use can be generated by modernising our understanding of technology and regarding technological functions as imposed properties rather than intrinsic ones (see also, Balmer, 2006). In previous work (Nightingale, 2004) science and technology were distinguished by their 'the direction of fit' (Searle, 1995) that relates to whether ideas are changed to fit the world, or the world is changed to fit ideas. As a first approximation, scientific ideas (theories, explanations etc) are meant to be true and the process of research involves changing these ideas until they match the world. Technologies on the other hand are meant to generate desired functions, and the process of innovation involves changing the world until it fits a (desired) idea of how it should function (Searle, 1995). The intentional level of ideas, desired behaviours and functions is therefore conceptually distinct from the intrinsic physics of the world, which is why technologies can have multiple functions.[41]

Technologies' (imposed) functions depend on people's understanding, while how well technologies perform those functions depends on the intrinsic properties of the technology and its interactions with

[41] The same compact disc, for example, can have multiple functions and can be used to store data or music, as well as stopping a hot coffee cup marking a table (Nightingale, 1998). While the intrinsic physics of a technology determines how well it can perform certain functions, it is the imposed function that defines what a technology is. This is why a safety valve is still a safety valve with the function of stopping explosions, even when it malfunctions (i.e., its intrinsic physics fails to perform the imposed function it was designed to perform) (Searle, 1995, p. 19).

the wider environment (which typically includes other socio-technical systems). Since neither technologies' functions nor how well they perform them, are solely determined by their intrinsic, physical properties, innovation cannot be an *event* where the artefact/function is discovered. Instead, innovation is a *process* of changing features of the world until they produce a desired behaviour. This tends to be a difficult, time consuming, inherently uncertain, knowledge intensive and costly process involving a number of steps and a range of technologies. The difficulties arise because theory is a weak guide to practice due to the complexity of the interactions of technological components (Pavitt, 1999; Rosenberg, 1986; Nelson, 1982), the inherent unpredictability of the starting materials (Nightingale, 2004) and the socially embedded nature of the knowledge that is required (MacKenzie, 1990; MacKenzie and Spinardi, 1996; Balmer, 2006). Consequently, technology should not be understood as only artefacts as it includes and can be defined as "all the knowledge, concepts, experimental processes, tangible and intangible artefacts and wider socio-technical systems that are required to recognise technical problems and to conceptualise, formulate, research, develop, test, apply, diffuse and maintain effective solutions to those problems".

This conception of technology provides a new way of understanding dual use in terms of *technological convergence* (Rosenberg, 1963, p. 423) where different downstream technologies share some of their upstream technological inputs.[42] In other words, different final products (bicycles and sewing machines, or prohibited weapons and vaccines) share some (but only some) of the same technologies and knowledge within their production processes (machine tools for bicycles and sewing machines, and modern biotechnology for vaccines and biological weapons). The remainder of this section explores the strengths and weaknesses of these two models of the dual use problem.

3.2. Governing things: dual use as a technology transfer problem

Framing dual use policy in terms of preventing the transfer of 'dangerous' research and technology to hostile states or non-state actors is the main way dual use policy is presented in current debates. This draws heavily on traditional governance models where the prevention and oversight of technology transfers has played an important role. By assuming that technological functions are fixed this way of thinking focuses attention on inventive events and cutting edge science. This has the advantage that policy making can focus on materials and pathogens that are well known to be dangerous, which, while providing useful guidance, has limits and can generate a false sense of security (IoM/NRC, 2006).

In particular, thinking of technical change this way substantially under-estimates both the difficulty of moving from an invention to a working technology and the costs of technology transfer (Nightingale, 2004; MacKenzie and Spinardi, 1996). This, in turn, means that policy-makers can over-estimate the ease with which it is possible to move from a pathogen to a weapon with the potential to harm more than a few people, and the even larger technical problems associated with developing biological weapons of mass destruction. In some instances these technical problems have been beyond the ability of even large state-based BW programs. For example, both the UK and US conducted open-air field tests on animals using aerosolised plague in the 1950s and were unable to get the technology to work (Leitenberg, 2005, p. 49).[43] This lack of attention to the difficulties involved in innovation can distort policy priorities—for example, by misrepresenting and overhyping the risks of bioterrorists developing WMD, or focusing on cutting edge research at the expense of older, well established forms of knowledge.[44]

Although considering technology or research as being inherently dangerous has the advantage that it allows it, in theory, to be assigned a definite risk category that can be entered into some form of cost-benefit type calculation to guide policy, it is not at all clear in practice how one defines 'dangerous' and how one draws boundaries around what is, and what is not, to be considered dangerous (Balmer, 2006). For example, it is hard to see how to

[42] Rosenberg originally used technological convergence to explain American industrialisation which he argued had not only involved growing specialisation, complexity and differentiation, but also the 'introduction of a relatively small number of broadly similar productive processes to a large number of industries. ... [specifically] the growing adoption of metal-using technology employing decentralised sources of power' (Rosenberg, 1963, p. 422).

[43] The genes that regulate the pathogenicity of *Yersina pestis* for example are extremely temperature sensitive, creating major engineering problems in their successful large scale weaponisation. WMD require large scale, state based programs involving technological capabilities that are beyond the capabilities of terrorist organisations (Leitenberg, 2005). Moreover, the cell-like organisational structures of terrorist groups is precisely the opposite of the information rich organisational structures most suitable for innovation of this type (Jackson, 2001).

[44] Similarly, it can lead policy makers to under-estimate the value of international treaties, particularly treaties with sophisticated verification architectures (MacEachin, 1998).

assess the relative costs of (a) putting the 1918 flu virus genome on the web, (b) highlighting the pathogenicity genes in the *Yersina pestis* genome, or (c) developing immune evasion technologies for gene therapy. Since the benefit of such research is also extremely difficult to quantify, a policy of weighing up costs, risks and benefits is of limited practical use when there is no agreed way of defining or comparing them (Royal Society, 1992).

The problem encountered here is not simply that definitions are not agreed in practice but that unambiguous definitions cannot be agreed in principle: 'dangerous' is not a descriptive term that denotes a property of something, but an expressive term that refers to how we think about the possible implications of the properties of something (Hopkins and Nightingale, 2006). Similar problems occur in labeling a technology 'risky' or 'beneficial'. While the intrinsic physical properties of a technology interact with its environment to generate the function that we regard as dangerous or risky, 'dangerousness' or 'riskiness' can never be *fully* defined in terms of those physical properties alone. Being context dependent, different people will rank the subjective terms in different ways, which complicates the policy process and has caused questions to be asked about the assignment of risk categories (Tuerlings and McLeish, 2004) and the objectivity and legitimacy of expert opinion in risk assessments of bioterrorism.

Despite these theoretical concerns, within the current policy discourse the dual use dilemma is mainly tackled by attempting to fix definitions that can categorise lists of pathogens or experiments. While this is eminently sensible, the difficulty of defining dangerousness does not go away: 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 the UK government, whilst others they considered as not being particularly dangerous given the UK's climate were included (McLeish and Nightingale, 2005). Moreover, fixed-definition or agent-specific/experiment-specific threat list approaches, while no doubt useful, will require constant updating because the scientific disciplines related to biological weapons development are advancing rapidly and proliferating through legitimate channels. For this reason, it is useful to consider them a tool rather than a solution, and to be aware of their limitations (IoM/NRC, 2006).

One of their potential limitations is a lack of flexibility and consequent inability to explore the context-dependence of 'dangerousness' to generate more sophisticated guidance about priorities. There is little benefit, for example, in adopting a '3G' approach – of guns, guards and gates – to protect pathogens on university campuses, if they can be easily sourced in the surrounding countryside. This lack of attention to context can also lead policy makers to overlook existing controls and adopt inappropriate, overly coercive measures.

Possibly the most important problem with policies directed towards controlling dangerous things is that if 'dangerous' is context dependent, then almost anything could be potentially dangerous. If one considers the potential advances that could be made in immunology and virology over the next few decades then it is hard to see how any research might *not* be regarded as *potentially* dangerous. In such a situation there is little inherent limit on the extent of controls, which combined with the inherent weaknesses of controls on things (that can be innovated around) and strong political pressure (for example, related to a public fear of bioterrorism) could result in policies that generate the worst of all possible worlds: Draconian controls that damage legitimate research and have no significant effect on security. Moreover, such controls can reduce the transparency needed to maintain an international regime based on trust, and impose further costs if they hinder the identification and treatment of natural outbreaks or deliberate releases.

3.3. Governing purposes: dual use as a technological convergence problem

Our second way of understanding dual use regards it as a particular subset of technological convergence whereby the same upstream technologies can have both hostile (military) and peaceful (civilian) downstream applications (Alic et al., 1992; Reppy, 1999).[45] Dual use, as the term is used in this paper, is a further subset that relates to technological convergence in the technology base that is used to produce both legitimate and prohibited technologies, (i.e. biotechnology is used to produce both vaccines and biological weapons). Because physical properties and functions do not necessarily match, technical change is understood as a *process* rather than an event, that involves intervening in the world until the intrinsic physics of a technology generates a

[45] This overlap between technological convergence and dual use is not novel. Ames and Rosenberg (1968) highlighted the how the establishment of the Enfield Arsenal in 1854 marked the beginning of the movement of mass production techniques from the USA to Europe. Indeed, Ames and Rosenberg note that 'Technical changes in gun making in the 19th century were a major source of new machine techniques; and industrialisation in the 19th century is overwhelmingly the history of the spread of machine making and machine using' (1968, p. 827).

desired effect/purpose/function.[46] As already noted, for complex technologies this can require a large amount of trial and error experimentation, knowledge integration, and infrastructure (Pavitt, 1999). The policy problem is therefore to direct technical change along socially beneficial rather than prohibited trajectories, by influencing the 'technological paradigms' (Dosi, 1982) that can be followed. This involves recognising and governing points of overlap and convergence along the different innovation processes in their use of artefacts, and links to socio-technical systems and personal intentions.

The substantial differences in the innovation processes that turn the same upstream technologies into prohibited or socially beneficial downstream technologies provide a range of opportunities for controls to hinder prohibited technical change, often at a lower cost, than Draconian controls on the transfer of 'dangerous' research. The potential web of controls is large because technology is not only comprised of tangible and intangible artefacts, it also involves formulating problems, conceptualising solutions and changing the world to reliably make it generate a desired function. As such, it is a non-trivial activity that typically requires a wide range of (spatially distributed) inputs and the co-ordination of a specialised division of labour over an extended period, making innovation an organisational and managerial problem as much as a technical one. While science is useful and can in some instances reduce the costs and time of technological development, it is not necessarily the most important, let alone the only, form of knowledge that is necessary *and can be governed*. Diseases were applied in hostile situations long before their exact modes of action were understood (Geissler and van Courtland Moon, 1999) as it is possible to know how to produce effects without knowing how those effects are produced.

Thinking about dual use policy in this way moves policy making away from notions of the inherent dangerousness of scientific research. Even the most 'dangerous' pathogens can be routinely experimented on quite safely within well-maintained and managed containment-laboratories.[47] Instead, policy should follow the General Purpose Criterion of Article 1 of the BWC and be directed at purposes rather than things. This will prevent policies being overtaken by changes in technology, and prevent regime violators innovating around controls. However, this flexibility comes at a cost, as governance measures that cover purposes do not provide clear guidance at the level of the artefact about what specifically is and what is not to be the subject of governance. The main problem is that because the purposes that are being controlled are imposed rather than intrinsic properties, they will always have the potential to "slip through your fingers" because (a) governance measures are operationalised around artefacts and their intrinsic properties, and (b) artefacts and their functions do not necessarily always coincide. Such governance measures are inherently problematic when new technologies are developed and when old technologies can be applied to new purposes. This slipperiness is one reason why artefact based governance has the potential to be both Draconian and ineffective and why operationalising the control of purposes will always be non-trivial.

However, while the governance of 'purposes rather than things' is non-trivial, it is not impossible. Because the focus of policy is not necessarily on controlling things as an end in itself, but rather as a means to control purposes, it implies a lighter touch in policy design in order to exploit the "strength of weak ties" (Pearson, 1993) to create cumulative webs of governance measures that put barriers in prohibited technology development processes while leaving others (relatively) unhindered. Developing such a web of controls will require a reassessment of the costs and benefits of existing governance measures and the implementation of new controls to address gaps in the current governance web, particularly in relation to international criminalisation and awareness-raising within the scientific community.

While many of the existing controls are prudent, such as controlling access to pathogens and sensitive technology, even the most Draconian controls will not stop determined proliferators from sourcing pathogens in nature or innovating around controls. Given that scientific knowledge is only one of a wide range of inputs required for innovation, a default position would probably be that legitimate scientific research (i.e. research not directed at forbidden purposes) should be unhindered, unless there is a good reason otherwise. This would make

[46] Collapsing the distinction between innovation and invention inappropriately focuses policy on cutting edge science. Regime violators are not necessarily interested in the most up to date technology, they are more interested in technologies that work, and are therefore likely to be well established. The value for regime violators of cutting edge research is likely to be more associated with equipment, experimental protocols and people trained to solve complex technical problems, than cutting edge research results.

[47] In interview one UK scientist discussed working with open Petri dishes containing live smallpox virus cultures in the 1960s. Scientists worked on the open bench without safety glasses, gloves or containment boxes. Researchers kept their lunch (typically sandwiches) uncovered on the bench next to the live samples and smoked while working, leaving their lit cigarettes on the side of the bench when they needed two hands to manipulate samples.

potential deviations from legitimate research trajectories easier to detect within a culture of openness where the scientific community takes a more active role in guarding against misuse.

A higher degree of responsibility and self-regulation within the scientific community will require education and awareness raising. Framing dual use in terms of technology transfer, and consequently framing the scientific community as naively transmitting dangerous knowledge and materials, is unlikely to enculture scientists to cooperate. On the other hand, framing dual use in terms of technology convergence allows scientists to perceive themselves as actors engaged in socially beneficial activities which could be misused and offers them an identity as 'guardians of science' in the fight against BW and bioterrorism, rather than the passive recipients of bureaucratic regulations.[48] In previous research (McLeish and Nightingale, 2005) we found that scientists in the UK were far more willing to become actively engaged with biosecurity governance, and were willing to devote considerable amounts of time to it, if they were seen as 'guardians' rather than 'naïve dupes' and if they recognised the controls as rational and effective.[49] However, the ability of scientists to effectively fulfil this role will depend on the security services building up their own internal technological capabilities, both to make decisions and to successfully interact with the wider scientific community in discussing emerging threats and their solution.

4. Discussion and conclusion

While it is important not to over-state the extent of the changes reviewed in this paper, they do represent an important new development and suggest an increasing interaction between science and security policy. The paper has argued that the changes are part of a wider evolution of the regime against the hostile use of disease that has been driven by an increased perception of threat and an increased appreciation of the potential misapplication of legitimate research. 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 (McLeish, 2004, McLeish and Nightingale, 2005). Given that initial reports suggest that they are already having an adverse impact on US science (Atlas, 2002, 2003; Gaudioso and Salerno, 2004), legitimate science policy questions are raised about the design and implementation of biosecurity policies and how they might be improved.

To assist policy makers in developing more effective policy, Section 2 contextualised these controls within a historical account of the anti-BW regime that it is neither divorced from, nor determined by changes in the wider world. It highlighted how national and international security legislation has covered scientific research since the banning of BW in the 1970s and the resulting shift towards the governance of technology. Research related to biological weapons for hostile purposes, for example, has been a serious criminal offence since the 1970s in the UK. This suggests that the popular notion that changes in governance are a simple internal response by the scientific community to an increased threat from bioterrorism since 2001 is implausible. Instead, the expansion of the security regime to increasingly address science reflects *ad hoc* responses by states to weaknesses in the BWC, inadequacies in export controls, incomplete implementation of the requirement under international law for domestic legislation and the failure to strengthen the BWC in 2001.

Section 3 examined the different ways in which biosecurity controls could be framed and highlighted how policies that understand dual use in terms of the transfer of inherently dangerous technology (materials or knowledge) have the potential to be both draconian and ineffective when applied to the life sciences even though they worked for nuclear technologies. An alternative framing of dual use, where it is understood in terms of technological convergence, was then introduced which focused on disrupting innovation processes rather than controlling artefacts. This highlighted how creating technologies that behave in predictable ways involves complex organisational processes, and becomes substantially more complex as one moves from dangerous pathogens, to weaponised pathogens capable of infecting several people, to WMD capable of infecting thousands. While terrorists may be able to generate mass *disruption* by inducing public fear and inappropriate policy responses (Sunstein, 2003), their limited technological capabilities, historical technological conservatism and inappropriate organisational structures suggest they are unlikely to develop WMD capabilities without the assistance of state based programs, which remain the major security concern. Just as linear models of innovation

[48] We are grateful to Dr. Tony Phillips, visiting fellow with the Harvard Sussex Program, for the term 'guardians of science'.

[49] Framing dual use controls in terms of technology transfer invoked a linear model of innovation that they recognised to be false, and therefore undermined their willingness to actively engage with new security measures.

under-estimate the risk, difficulty and costs of innovation in science policy, they also over-estimate the risks, difficulty and costs of innovation in security policy.

Thinking about biosecurity policy in terms of technological convergence suggests some new avenues for thinking about security policy. Within the broader science and technology policy field there is a considerable body of knowledge about the conditions that contribute towards successful processes of innovation (Nelson, 1962; Rothwell, 1977; Pavitt, 1999; Hobday, 1998) that can be implemented to direct technical change along socially acceptable trajectories (Dosi, 1982). In conclusion, we would suggest that while this body of knowledge can be used to *reduce* the risks, uncertainties, redesign feedback-loops, and costs of innovation (see Nightingale, 2000) its application can be *reversed* to highlight methods of *increasing* those risks etc., to direct innovation paths away from trajectories prohibited by international law (Dosi, 1982). In doing so, it generates a number of policy implications that are broadly in line with the findings of the IoM/NRC (2006) committee:

First, since the science policy community has established that innovation is encouraged by widespread institutional co-operation (Rothwell, 1977), innovation processes could be disrupted by encouraging non-co-operation. Given the shared culture of the scientific community and their historically important role in BW development, they could be encouraged to take on an active role as 'guardians of science' to help prevent proliferation. This will require greater investments in training, education and awareness-raising within the scientific community about the potential for research to contribute towards the production of weapons that are banned under international law for violating the norms of *distinction* between military and civilian targets, and *proportionality*, in the unnecessary psychological and physical suffering they cause.

Secondly, research has shown (Hobday, 1998) that the development of the sort of infrastructure needed to produce complex technologies such as a biological weapon or complex technological systems such as a BW research program is extremely difficult, time consuming and costly. Drawing on such research would allow policy makers should adopt a more nuanced approach to risk and guide the security community to focus on how innovation processes diverge, thereby providing opportunities for new governance measures that enhance security without causing extensive disruption to legitimate research.

Thirdly, the science policy literature has shown (Balmer, 2006; Nightingale, 2004) how technical change involves intentional choices that are influenced by and interact with wider society. A clear normative articulation of acceptable and unacceptable behaviour would therefore contribute towards improved governance. Currently there is a lack of international criminalisation of individual activity in relation to biological weapons production that might allow actors to rationalise their choices. The adoption of a criminalisation measure at the international level would provide a new and very clear articulation of the universal condemnation at the heart of the regime while also avoiding the problems of harmonising national laws. While self-governance measures and national criminal legislation play important roles in governing intentions, they are a complement rather than a substitute for international legal measures. As well as problems of harmonising various provisions regarding the definition of crimes, the rights of the accused, judicial assistance, etc., national criminal statutes (which are still poorly implemented) do not convey the universal condemnation implicit in international criminal law.

The present lack of international criminalisation of specific acts involving chemical and biological weapons is therefore a significant hole within the potential web of controls that could be used to counter BW. However, a draft convention that would confer on national courts the jurisdiction over individuals present in their national territory regardless of their nationality or official position who order, direct or knowing lend substantial assistance to the use of biological weapons anywhere has been proposed by the Harvard Sussex Program on Chemical and Biological Weapons. Adoption of this convention would create a new dimension of constraint by holding individual offenders (regarded under the Convention as *hostes humani generis*—'enemies of all humanity') responsible and punishable should they be found on the territory of any State that supports the Convention (Meselson and Robinson, 2002a). This would substantially strengthen the web of controls by further institutionalising the regime's norm and by providing an overarching umbrella for other measures directed at purposes.[50]

Fourthly, research has shown that substantial capabilities are needed by organisations to effectively engage with the scientific community (Rothwell, 1977; Pavitt, 1999). Given the increasing overlap between science and security policy, this suggests the security community will need to develop improved technological capabilities to monitor and respond to changes in science. This is likely

[50] A range of other measures that could also improve security have already been developed (see for example, Littlewood, 2004, 2005; Guillemin, 2005; Meselson and Robinson, 2002b; MacEachin, 1998; Wheelis and Dando, 2002; Pearson, 1993; NRC, 2005; Meselson, 2000).

to become more important in the future as advances in areas such as immunology and pathogenesis significantly complicate biosecurity.

Fifthly, many of the benefits of interacting with the research system do not come from academics providing the 'answer', but from them providing new ways of understanding and thinking about complex problems (Pavitt, 1999). As Moodie (2004, p. 51) argues 'concepts shape our constructs of reality, and they can prompt a sense of new opportunities with respect to what can be done to address major challenges. In other words, it both opens up new policy options and promotes either the identification of new policy tools or the application of existing tools in novel ways'. In this paper we have suggested that the security community might benefit from thinking about dual use in new ways.

Finally, and as an example of the last point, thinking of dual use in terms of technological convergence raises an important question about the risks and benefits associated with the expansion of biodefence research within current biosecurity policy that may be usefully addressed by future research.[51] Biodefence research has a dual use potential, in that it is necessary to understand how to develop biological weapons if one is to defend against them. While this is permitted by the BWC, it unfortunately creates exactly the technological capabilities that run counter to anti-proliferation policy (Meselson and Robinson, 2002b). While these capabilities are intended to be applied to peaceful defence, their dual use nature means that they also represent a considerable risk (Wheelis and Dando, 2002). At present, more than 300 institutes and 12,000 individuals in the US have access to pathogens historically associated with bioweapons (Schwellenback, 2005). Worryingly, analysis of the principal investigators of NIAID grants awarded between 2001 and 2005 to study the six priority biodefence pathogens suggests that 97% of them are new to the field, considerably increasing the number of people possessing the necessary technical knowledge needed to work with dangerous pathogens (ibid). Moreover, unless conducted in a transparent manner such programs they have the potential to undermine the international trust that has been a key factor in the success of the BWC (Walker, 2003). Given the very substantial sums of money invested in biodefence, there is a need to critically examine the implicit policy assumption that biodefence increases security and reduces risk exposure (Corneliussen, 2006).

In conclusion, this paper suggests that Meselson (2000) was correct in highlighting that biological weapons present a major policy problem for science, and that new governance mechanisms will be needed to prevent what he describes as a 'species threatening' problem. However, while Meselson highlights the potential dangers of advances in technology and biological sciences, he is not a technological determinist, and he explicitly highlights the possible hostile application of advances in biological science presents a fork in the road rather than a conclusion. Given that advances in biology are likely to continue, science policy is going to have to continue to address security issues, and further research will be necessary to ensure that the dual use dilemma is properly addressed and the benefits of security restrictions are balanced against their social costs on legitimate activities.

[51] Total NIH funding for biodefence has increased from $25 m (FY 2001), to a peak at $1748 m (FY 2003) before falling slightly to $1600 m in 2004 (Fauci, 2005; Harris and Steinbruner, 2005). For comparison the *total* research funding of the UK Medical Research Council (2004) was approximately $500 m. The majority of the NIH funding (2003) went to the National Institute of Allergy and Infectious Diseases (NIAID) where 50 biodefence initiatives were developed. New initiatives include the construction of a series of National Biocontainment Laboratories built to Biosafety Level 4 standards, together with nine Regional Biocontainment Laboratories with Biosafety Level 3 facilities. NIAID has also funded eight Regional Centres of Excellence for Biodefense and Emerging Infectious Diseases Research (Fauci, 2005). Increases in funding have potentially shifted the direction of research towards pathogens with potential hostile use, as grants for research on BW agents have risen 1500% from "33 between 1996 and 2000, to almost 500 between 2001 and January 2005" (Harris and Steinbruner, 2005, p. 1).

Acknowledgements

The authors are grateful to two anonymous referees and Prof. Julian Perry Robinson and Dr. Tony Phillips for insightful comments on previous versions of this paper. Usual disclaimers apply.

References

Acha, V.L., 2002, Framing the past and future: the development and deployment of technological capabilities by the oil majors in the upstream petroleum industry. Unpublished D.Phil. Thesis. University of Sussex, UK.

Alic, J.A., 1993. Technical knowledge and technology diffusion: new issues for US Government Policy. Technology Analysis and Strategic Management 5 (4), 369–383.

Alic, J., Branscomb, L., Brooks, H., Epstein, G., Carter, A., 1992. Beyond Spin-off: Military and Commercial Technologies in a Changing World. Harvard Business School Press, Boston.

Altman, S., et al., 2005. An open letter to Elias Zerhouni. Science 307 (5714), 1409–1410.

Ames, E., Rosenberg, 1968. The Enfield arsenal in theory and history. Economic Journal 78, 827–842.

Archibugi, D., 2001. Pavitt's taxonomy sixteen years on: a review article. Economics of Innovation and New Technology 10 (5), 415.
Arnone, M., 2004. New survey confirms sharp drop in applications to US colleges from foreign graduate students. The Chronicle of Higher Education. March 4.
Atlas, R.A., 2001. Bioterrorism before and after September 11. Critical Reviews in Microbiology 27, 355–379.
Atlas, R.A., 2002a. National security and the biological research community. Science 298, 753–754.
Atlas, R.M., 2002b. National security and the biological research community. Science 298, 753–754.
Atlas, R.M., 2003. Science publishing in the age of bioterrorism. Academe 89 (5), 14–18.
Bacon, 1609. Daedalus, or the Mechanik. In: Of the Wisdom of the Ancients. Deer, Brighton (Chapter 19).
Balmer, B., 2002. Biological weapons: the threat in historical perspective. Medicine, Conflict and Survival 18 (2), 120–137.
Balmer, B., 2001. Britain and Biological Warfare: Expert Advice and Science Policy 1930–65. Palgrave, Basingstoke.
Balmer, B., 2006. A Secret formula, a rogue patent and public knowledge about nerve gas. Social Studies of Science 36 (5), 691–722.
Balmer, B., 1997. The drift of biological weapons policy in the UK 1945–65. The Journal of Strategic Studies 20 (4), 115–145.
Bozeman, B., 2000. Technology transfer and public policy: a review of research and theory. Research Policy 29, 627–655.
Braithwaite, J., 1993. Beyond positivism: learning from contextual integrated strategies. Journal of Research in Crime and Delinquency 30, 383–399.
Braithwaite, J., 1994. A Sociology of modelling and the politics of empowerment. British Journal of Sociology 45 (3), 445–479.
Braithwaite, J., 2002. Restorative Justice and Responsive Regulation. Oxford University Press, New York.
Braithwaite, J., Drahos, P., 2000. Global Business Regulation. Cambridge University Press.
Breithaupt, H., 2000. Toxins for terrorists do scientists act illegally when sending out potentially dangerous material? EMBO Reports 1 (4), 298–301.
Broad, W., 2002. US is tightening rules on keeping scientific secrets. The New York Times, 17 February.
Byers, M., 2004. Policing the high seas: the proliferation security initiative. American Journal of International Law 98 (3), 526–545.
Cameron, G., 1999. Multi-track microproliferation: Lessons from Aum Shinrikyo and Al Qaeda. Studies in Conflict and Terrorism 22 (4), 277–309.
Cello, A., Paul, A.U., Wimmer, E., 2002. Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. Science 297, 1016–1018.
Chyba, C., Greninger, A., 2004. Biotechnology and bioterrorism: An unprecedented world. Survival 46 (2), 143–162.
Cochrane, R.C., 1978. The National Academy of Sciences: The First Hundred Years, 1863–1963. National Academy of Sciences, Washington, DC.
Corneliussen, F., 2006. Adequate regulation, a stop-gap measure, or part of a package? Debates on codes of conduct for scientists could be diverting attention away from more serious questions. EMBO Reports 7, 50–54.
Council of Graduate Schools (CGS), 2004. Council of Graduate Schools Finds Decline in New International Graduate Student Enrolment for the Third Consecutive Year. 4 November. Available at: http://www.cgsnet.org/.
Cowan, R., Foray, D., 1995. Quandaries in the economics of dual technologies and spillovers from military to civilian research and development. Research Policy 24 (6), 851–868.
Cozzavelli, N.R., 2003. PNAS policy on publication of sensitive material in the life sciences. Proceedings of the National Academy of Sciences United States of America 100, 1463.
Danchin, A., 2002. Not every truth is good. The dangers of publishing knowledge about potential bioweapons. EMBO Reports 3, 102–104.
Defense Science Board, 2000. Protecting the Homeland: Report of the Defense Science Board. Washington, DC.
Dosi, G., 1982. Technological paradigms and technological trajectories: a suggested interpretation of the determinants and directions of technical change. Research Policy 11 (3), 147–162.
Ellis, J., 2003. The best defense: counterproliferation and US national security. The Washington Quarterly 26 (2), 115.
Enserink, M., Kaiser, J., 2005. Has bioterrorism gone overboard? Science 307, 1396–1398.
Finkel, E., 2001. Engineered mouse virus spurs bioweapon fears. Science 291, 585.
Fourth Review, 1996, Fourth Review of the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological Biological and Toxin Weapons and on their Destruction, Final Document, Geneva, 25 November-6 December 1996, BWC/CONF.IV/9.
Fraser, C.M., Dando, M.R., 2001. Genomics and future biological weapons: the need for preventive action by the biomedical community. Nature Genetics (29), 253–256.
Freeman, C., 1982. The Economics of Industrial Innovation. Pinter.
Gaudioso, J., Salerno, R.M., 2004. Biosecurity and research: minimizing adverse impacts. Science 304 (5671), 687.
Geissler, E., van Courtland Moon, J.E. (Eds.), 1999. Biological and Toxin Weapons: Research, Development, and Use from the Middle Ages to 1945, SIPRI Chemical and Biological Warfare Study No. 18. Oxford University Press, Oxford.
Gibbons, M., Johnston, R., 1974. The roles of science in technological innovation. Research Policy 3 (3), 220–242.
Gilbert, N., 2007. All postgraduate visas to require security vetting. Research Research.
Greenwood, C., 2000. The law of war (International Humanitarian Law). In: Evans, M.D. (Ed.), International Law. Oxford University Press, pp. 769–823 (Chapter 25).
Guillemin, J., 2005. Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism. Columbia University Press, New York.
Harris, E.D., Steinbruner, J.D., 2005. Scientific Openness and National Security After 9/11. The CBW Conventions Bulletin 67, 1–3.
Hasenclever, A., Mayer, P., Rittberger, V., 1997. Theories of International Regimes, Cambridge Studies in International Relations, No. 55. Cambridge University Press.
Hicks, D., 1995. Published papers, tacit competencies and corporate management of the public/private character of knowledge. Industrial and Corporate Change, vol. 4, No. 2, p. 401.
Hobday, M., 1998. Product complexity, innovation and industrial organisation. Research Policy 26, 689–710.
Hopkins, M.M., Nightingale, P., 2006. Strategic risk-management using complementary assets: organizational capabilities and the commercialisation of human genetic testing in the UK. Research Policy 35 (3), 355–374.
Institute of Medicine and the National Research Council, Committee on Advances in Technology and the Prevention of their Application

to Next General Biowarfare Threats, 2006. Globalization, Biosecurity and the Future of the Life Sciences. National Academies Press, Washington, DC.

Jackson, B., 2001. Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption. Studies in Conflict and Terrorism 24 (3).

Jackson, R., Ramsay, A., Christensen, C., Beaton, S., Hall, D., Ramshaw, I., 2001. Expression of mouse interleukin-4 by recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. Journal of Virology 75, 1205–1210.

Joyner, D., 2004. The Proliferation Security Initiative and International Law. Center for International Trade and Security, CITS Briefs, Athens, Georgia.

Kahn, A.H., 2004. Biodefense research: can secrecy and safety coexist? Biosecurity and Bioterrorism: Biodefence Strategy, Practice and Science 2 (2), 81(5)–85(5).

Kellman, B., 2004. Criminalization and control of WMD proliferation: The Security Council acts. The Nonproliferation Review 11 (2), 142–161.

Kellman, B., 2001. Biological terrorism: legal measures for preventing catastrophe. Harvard Journal of Law and Public Policy 24 (2), 457–462.

Kline, S.J., Rosenberg, N., 1986. An overview of innovation. In: Landau, R., Rosenberg, N. (Eds.), The Positive Sum Strategy: Harnessing Technology for Economic Growth. National Academic Press, Washington, DC.

Koblentz, G., 2003. Pathogens as weapons: The international security implications of biological warfare. International Security 28 (3), 84–122.

Krasner, S. (Ed.), 1983. International Regimes. Cornell University Press, New York.

Leitenberg, M., 2001. Biological weapons in the twentieth century: a review and analysis. Critical Reviews in Microbiology 27, 267–320.

Leitenberg, M., 2005. Assessing the Biological Weapons and Bioterrorism Threat. Strategic Studies Institute, US Army War College.

Lentzos, F., 2006. Rationality, risk and response: a research agenda for biosecurity. BioSocieties 1, 453–464.

Littlewood, J., 2005. The Biological Weapons Convention: A Failed Revolution. Ashgate, London.

Littlewood, J., 2004. Managing the biological weapons problem: from the individual to the international. WMD Commission. Paper No. 14.

MacEachin, D.J., 1998. Routine and challenge: two pillars of verification. The CBW Conventions Bulletin: Quarterly Journal of the Harvard Sussex Program on CBW Armament and Arms Limitation 39, 1–3.

MacKenzie, D., 1990. Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance. MIT Press, Cambridge, MA.

MacKenzie, D., Spinardi, G., 1996. Tacit knowledge and the uninvention of nuclear weapons. In: MacKenzie, D. (Ed.), Knowing Machines: Essays on Technical Change. MIT Press, Cambridge, MA.

Malakoff, D., 2003. Researchers urged to self-censor sensitive data. Science 299, 321.

Martin, B., Nightingale, P., 2000. Introduction. In: Martin, B., Nightingale, P. (Eds.), The Political Economy of Science, Technology and Innovation. Edward Elgar.

Martin, S.B., 2002. The role of biological weapons in international politics: the real military revolution. Journal of Strategic Studies 25 (1), 25, 1, 63.

McLeish, C., Nightingale, P., 2005. The Impact of Dual Use Controls on UK Science: Results from a Pilot Study, SWEPS 132. SPRU, Brighton.

McLeish, C., 2002. Accommodating bio-disarmament to biotechnological change. Unpublished D.Phil. Thesis. SPRU, University of Sussex, Brighton.

McLeish, C., 2004. A background note on dual use technologies: can technology studies inform the dual use debate? In: Paper Presented at 21st Pugwash CBW Workshop: The BWC New Process and the Sixth Review Conference, Geneva, Switzerland, December 4–5, 2004. SPRU, Brighton.

Merton, R., 1973. The Sociology of Science. University of Chicago Press, Chicago.

Meselson, M., Robinson, J.P., 2002a. A draft convenion to prohibit biological and chemical weapons under international criminal law. In: Yepes-Enríquez, R., Tobassi, L. (Eds.), Treaty Enforcement and International Co-operation in Criminal Matters with Special Reference to the Chemical Weapons Convention. TMC Asser Press, The Hague.

Meselson, M., Robinson, J.P., 2002b. Preventing the hostile use of biotechnology: the way forward now. The CBW Conventions Bulletin 57, 1–2.

Meselson, M., 2000. Averting the hostile exploitation of biotechnology. The CBW Conventions Bulletin (48), 16–19.

Molas-Gallart, J., Robinson, J.P. 1997. Assessment of dual-use technologies in the context of European security and defence. Report for the Scientific and Technological Options Assessment (STOA), European Parliament.

Molas-Gallart, J., 1996. Developing dual-use technology transfer methodologies: a taxonomy of policy alternatives. Report Prepared for the National Engineering Laboratory, SPRU, Brighton.

Molas-Gallart, J., 2002. Coping with dual-use: a challenge for European research policy. Journal of Common Market Studies 40, 155–165.

Molas-Gallart, J., 1997. Which way to go? Defense technology and the diversity of 'dual use' technology transfer. Research Policy 26, 367–385.

Molas-Gallart, J., 2000. The political and economic context of European defence R&D. SPRU Electronic Working Paper Series No. 52. University of Sussex.

Moodie, M., 2004. Confronting the biological and chemicals challenge: the need for an "intellectual infrastructure". The Fletcher Forum of World Affairs, vol. 28, Winter.

Müller, H., 1995. The internationalisation of principles, norms and rules of governments: the case of security regimes. In: Ritterger, V., Mauer, P. (Eds.), Regime Theory and International Relations. Clarendon Press, Oxford.

Musser, G., 2001. Better killing through chemistry. Scientific American 285, 20–21.

National Academies of Sciences, National Academy of Engineering, Institute of Medicine, 1982. Scientific Communication and National Security. A Report Prepared by the Panel on Scientific Communication and National Security Committee on Science, Engineering, and Public Policy. US National Academy Press, Washington DC [The Corson Report]. Available at: http://www.nap.edu/books/0309033322/html/.

National Research Council of the National Academies of Sciences. Committee on Research, Standards and Practices to Prevent the Destructive Application of Biotechnology, 2004. Biotechnology Research in an Age of Terrorism: Confronting the Dual use Dilemma. US National Academy of Sciences, Washington, DC.

National Research Council of the National Academies of Sciences. Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats, 2005. An International Perspective on Advancing Technologies and Strategies for Managing Dual-Use: A Report from a Workshop. National Research Council, Washington, DC.

Nature Editorial, 2003. Statement on the consideration of biodefence and biosecurity. Nature 421.

Nelson, R.R. (Ed.), 1962. The Rate and Direction of Inventive Activity. Princeton University Press, Princeton.

Nightingale, P., 1998. A cognitive model of innovation. Research Policy 27, 687–709.

Nightingale, P., 2000. The product–process–organisation relationship in complex development projects. Research Policy 29, 913–930.

Nightingale, P., 2004. Technological capabilities, invisible infrastructure and the un-social construction of predictability: the overlooked fixed costs of useful research. Research Policy 33 (9), 1259–1284.

Noble, R.K., 2006. Secretary-general's foreword. In: Bio-terrorism Incident Pre-planning and Response Guide. ICPO-INTERPOL, Lyon, France.

Oosthuizen, G., Wilmshurst, E., 2004. Terrorism and weapons of mass destruction: United Nations Security Council Resolution 1540. Chatham House Briefing Paper 04/01.

Pavitt, K., 1984. Sectoral patterns of technical change: towards a taxonomy and a theory. Research Policy 13, 343–373.

Pavitt, K., 1999. Technology, Management and Systems of Innovation. Edward Elgar, Cheltenham.

Pearson, G.S., 1993 (Spring). Prospects for chemical and biological arms control: the web of deterrence. Washington Quarterly 16 (2), 147–148.

Purver, R., 2002. Chemical and Biological Terrorism: the Threat According to the Open Literature. Canadian Security and Intelligence Service.

Reppy, J., 1999. Dual-use technology: back to the future? In: Markusen, A., Costigan, S. (Eds.), Arming the Future: A Defense Industry for the 21st Century. Council on Foreign Relations Press, New York, NY.

Reppy, J., 2006. Managing Dual-Use Technology in an Age of Uncertainty. The Forum 4 (1), Article 2. Available at: http://www.bepress.com/forum/vol4/iss1/art2.

Roberts, B., 1995. Rethinking export controls on dual-use materials and technologies: From trade restraints to trade enablers. The Arena (2).

Robinson, J.P., 1997. Controlling dual-use biotechnology: the crucial role of national measures. In: Paper for the 8th Pugwash Study Group on Implementation of the CBW Conventions Workshop, Geneva, September 20–21, 1997. SPRU, Brighton.

Robinson, J.P., 1992. The Australia Group: a description and assessment. In: Brauch, H., van der Graaf, H., Grin, J., Smit, W. (Eds.), Controlling the Development and Spread of Military Technology: Lessons from the Past and Challenges for the 1990s. VU University Press, Amsterdam.

Rosenberg, N., 1963. Technological change in the machine tool industry, 1840–1910. Journal of Economic History 23, 414–443.

Rosenberg, N., 1982. Inside the Black Box: Technology and Economics. Cambridge University Press, Cambridge.

Rosengard, A., Liu, Y., Nie, Z., Jimenez, R., 2002. Variola virus immune evasion design: expression of a highly efficient inhibitor of human complement. Proceedings of the National Academy of Sciences 99, 8808.R–8813.R.

Rothwell, R., 1977. The characteristics of successful innovators and technically progressive firms. R&D Management 7 (3), 191–206.

Royal Society, 1992. Risk: Analysis, Perception and Management. Royal Society, London.

Schwellenback, N., 2005. Biodefense: A Plague of Researchers. Bulletin of the Atomic Scientists 61 (3), 14.

Searle, J.R., 1995. The Construction of Social Reality. Allen Lane.

Sunstein, C.R., 2003. Terrorism and probability neglect. Journal of Risk and Uncertainty 26, 121–136.

The Hague, 1923. Draft rules of aerial warfare. Never Adopted.

Tuerlings, E., McLeish, C., 2004. Is risk assessment a useful method to govern dual use research? In: Paper Presented at 21st Pugwash CBW Workshop: The BWC New Process and the Sixth Review Conference, Geneva, Switzerland, December 4–5, 2004. SPRU, Brighton.

United Kingdom of Great Britain and Northern Ireland, 1974. The Biological Weapons Act.

United Kingdom of Great Britain and Northern Ireland, 2003. Export of Goods, Transfer of Technology and Provision of Technical Assistance (Control) Order.

United Kingdom of Great Britain and Northern Ireland, 2001. Anti Terrorism Crime and Security Act.

United Kingdom of Great Britain and Northern Ireland, 2001. Paper Prepared as part of Background Paper On New Scientific And Technological Developments Relevant To The Convention On The Prohibition Of The Development, Production And Stockpiling Of Bacteriological (Biological) And Toxin Weapons And On Their Destruction, BWC/CONF. V/4/Add.1.

United Kingdom of Great Britain and Northern Ireland, 2002. Export Control Act.

United Nations General Assembly, 1977. Economic and social consequences of the armaments and its extremely harmful effects on world peace and security. Report of the Secretary General, A/32/88 August 12, 1977.

United Nations Security Council, 1992. Note by the President of the Security Council. January 31, S/23500.

United Nations Security Council Resolution 1540, 2004. Non-proliferation of weapons of mass destruction. S/RES/1540.

United States of America, 1985. National Policy on the Transfer of Scientific, Technical and Engineering Information. NSDD 189.

United States of America, 1989. The Biological Weapons Anti Terrorism Act.

United States of America, 1996. Antiterrorism and Effective Death Penalty Act.

United States of America, 1996. Illegal Immigration Reform and Immigrant Responsibility Act.

United States of America, 2001. Paper Prepared as part of Background Paper on New Scientific and Technological Developments Relevant to the Convention on The Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction. BWC/CONF.V/4.

United States of America, 2001. Uniting and Strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act.

United States of America, 2002. Enhanced Border Security and Visa Entry Reform Act.

United States of America, 2002. Public Health Security and Bioterrorism Preparedness and Response Act.

United States of America, 2004. Intelligence Reform and Terrorism Prevention Act.

Walker, W., 2003. Reflections on transparency and international security. In: Zarimpas, N. (Ed.), Transparency in Nuclear Warheads and Materials: The Political and Technical Dimensions. Oxford University Press (Chapter 1).

Wallerstein, M.B., 2002. Science in an age of terrorism. Science 297, 2169.

Wheelis, M., Dando, M., 2002. On the brink: biodefence, biotechnology and the future of weapons control. The CBW Conventions Bulletin 58, 3–7.

Wilkie, T., 1993. Foreign students to be vetted, Independent (London), March 16, p. 1.

Zilinskas, R.A., 1999. Iraq's biological weapons: the past as future? In: Lederberg, J. (Ed.), Biological Weapons: Limiting the Threat. MIT Press, Cambridge, MA.