

## Possibilities, Intentions and Threats: Dual Use in the Life Sciences Reconsidered

Koos van der Bruggen

Received: 27 October 2010 / Accepted: 3 February 2011 / Published online: 17 February 2011  
© The Author(s) 2011. This article is published with open access at Springerlink.com

**Abstract** Due to the terrorist attacks of 9/11 and the anthrax letters of a few weeks later, the concept of dual use has spread widely in the life sciences during the past decade. This article is aimed at a clarification of the dual use concept and its scope of application for the life sciences. Such a clarification would greatly facilitate the work of policymakers seeking to ensure security while avoiding undesirable interventions of government in the conduct of science. The article starts with an overview of the main developments in life sciences in relation to dual use. This is illustrated by discussions on synthetic biology and dual use. The findings lead to a reconsideration of the dual use concept. An area in need of further attention is to what extent threats and intentions should have impact on the definition of dual use. Possible threats are analyzed against the background of the phenomenon of securitization of health care and life sciences: considering these sectors of society in security terms. Some caveats that should be taken into account in a dual use policy are described. An acceptable, adequate and applicable definition of the dual use concept could help researchers, universities, companies and policy makers. Such a definition should build upon, but go beyond, the view developed in the influential Fink-report, which concentrates on the so-called ‘experiments of concern’, e.g. experiments that enhance the virulence of pathogens (National Research Council of the National Academies 2004) It will be argued that—in addition to these more technical aspects—a definition of dual use should include the aspect of threats and intentions.

**Keywords** Dual use · Biosecurity · Biological weapons · Threat · Securitization

---

K. van der Bruggen (✉)  
Department Philosophy, Faculty of Technology, Policy and Management, Delft University  
of Technology, P.O.Box 5015, 2600 GA Delft, The Netherlands  
e-mail: k.vanderbruggen@hetnet.nl

## Life Sciences, Biological Weapons and Dual Use

Dual use is not a concept that is unique for the life sciences. The (possibility of) dual use is as old as engineering and designing. Literally dual use means nothing more and nothing less than that a certain activity or a certain object can be applied in at least two ways. This is the case with almost everything that has been designed or developed, but also with objects that are not human made, like natural herbs. To give some examples: a kitchen knife can be used to cut, but also sometimes as an alternative for a screw driver and indeed also to stab someone.<sup>1</sup> Palliative pills are meant to alleviate pain, but if someone takes enough of these pills they can be used for committing suicide. This list can be continued endlessly. Almost every artefact and many natural products can be applied in a dual or even multiple use way. The dual or multiple ways an artefact can be used are not always intended by the designer. A screwdriver is not designed to stab a person. In pharmaceutical research unexpected or unintended effects of medicines also can lead to dual use. Sometimes the original function even is displaced by the unintended one. A well-known example is the Viagra pill. This pill had been designed against angina pectoris, but is now used for almost 100% to solve erection problems.

Although serendipity surely is an interesting phenomenon in (life) sciences most scientists and engineers do not spend a lot of time on thinking about the unintended or unexpected side-effects that can occur when their products are used (van Andel 1994).<sup>2</sup> Even less they think of intended misuse. Making scientists, engineers and other designers aware of the possible misuse of their 'brainchild' is the main goal of the dual use policy that has been developed in the life sciences during the past years.

Based on the intention of the engineers and designers some distinctions can be made when declaring an artefact, an activity or a natural product as dual use. If the starting point is the military field, dual use is a concept indicating that new technological developments in the military field are also useful for non-military purposes. History shows some well known examples of this spin-off effect of military technology. Areas of spin-off include variable fields as communications, fuels, weather observation, power sources, protective clothing, and displays.

The concept of dual use that is at stake in present day discussions refers to (civil) products and technologies that can be used for beneficial purposes as well as for malicious purposes. As was said above this possibility of dual use of artefacts and of knowledge is possible with almost everything that is designed or produced. But in the present situation the most important application of the concept of dual use is related to weapons of mass destruction (WMD). As nuclear weapons are the most important of the WMD the concept was first applied in debates about the risk of misuse of nuclear technology. The concept of dual use in relation to nuclear weapons is most significant because of the regime of arms control. Inspections of the International Atomic Energy Agency (IAEA) are mainly directed at discovering intended or perhaps unintended activities of countries that can be seen as a breach of

<sup>1</sup> In practice artefacts are often not just dual use, but even multi-use.

<sup>2</sup> The Dutch author Pek van Andel belongs to the few scientists who wrote about the phenomenon of serendipity.

the Non Proliferation Treaty (NPT). Because of this link with the NPT states are the main actors that IAEA focuses upon, as is illustrated by the recent discussions about Iran and North Korea. But of course the risks of (nuclear) terrorism have not gone unnoticed by IAEA. In its mid term strategy for the period 2006–2011 IAEA has as one of its goals to “develop a comprehensive set of recommendations and guidelines for the international community, for the prevention, detection and response to acts of nuclear terrorism or other malicious acts, along with an appropriate review process” (IAEA 2006).

How is the dual use concept introduced and applied in relation to the life sciences? To gain insight in this question it is useful to start with describing the arms control context of biological weapons. This context is determined by the Biological and Toxin Weapons Convention (BTWC 1972). The BTWC was signed in 1972 and came into force in 1975. In those years BTWC was one of a greater number of arms control agreements during the Cold War period. The BTWC became possible—as Fidler and Gostin write—when the United States decided unilaterally to terminate its offensive program on biological weapons (Fidler and Gostin 2008, p. 47). The Soviet Union and other main powers followed. And so the first treaty that required real disarmament came into being.<sup>3</sup> The main article of the BTWC is article I:

Each State Party to this Convention undertakes 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.

Has the concept of dual use been an important element of the Convention? This was not the case until after the anthrax attacks of 2001. The words “dual use” do not appear in the text of the Convention nor in any of the final declarations of the six review conferences that have been organized since 1980. However, during the Sixth Review Conference (2006) explicit attention was given to what is called the misuse of biotechnology: “The Conference recognizes that while recent scientific and technological developments in the field of biotechnology would increase the potential for cooperation among States Parties and thereby strengthen the Convention, they could also increase the potential for the misuse of both science and technology” (Final Document Sixth Review Conference BTWC 2006, p. 19). The Conference decides to contribute one of the intersessional meetings to “Oversight, education, awareness raising, and adoption and/or development of codes of conduct with the aim of preventing misuse in the context of advances in bio-science and bio-technology research with the potential of use for purposes prohibited by the Convention” (Final Document Sixth Review Conference BTWC 2006, p. 25). In 2008 an Expert Meeting and an Intersessional Meeting of States

---

<sup>3</sup> Other treaties, such as the Strategic Arms Limitation Talks (SALT) agreements on nuclear weapons, did not go further than determining maximum numbers of weapons or missiles.

Parties were organized about the risks of misuse of biotechnology. In a report which synthesizes the discussions of the Expert Meeting 2008 the concept of dual use is mentioned in relation to the development of codes of conduct (Document BWC/MSP 2008, p. 7–8). Dual use is linked to three different words: biological agents or toxins, potential (of research) and directly to research. These different ways to apply dual use indicate that—even on the level of state parties of the BTWC—dual use is not an unequivocal concept. This can be illustrated by the recent discussions on the dual use character of synthetic biology.

## Synthetic Biology and Dual Use

It is remarkable that dual use was seen as an important issue almost from the beginning of the development of synthetic biology (De Vriend 2006, p. 54–57). What is the dual use risk of synthetic biology? Tucker and Zilinskas argue that “at present, the primary threat of misuse [of synthetic biology] appears to come from state-level biological warfare programs”. They refer to former Soviet scholars who could be engaged in such projects. But at the same page they state that these developments are “extremely unlikely” (Tucker and Zilinskas 2006, p. 38). Tucker and Zilinskas point to other risks: one of the possible scenarios for the deliberate misuse of synthetic biology involves a “lone operator,” such as a highly trained molecular biologist who develops an obsessive grudge against certain individuals or groups (or society as a whole) (Tucker and Zilinskas 2006, p. 17). The other risk comes from so called biohackers, e.g. college kids who are eager to demonstrate their technological abilities (Tucker and Zilinskas 2006, p. 18). The growth of the number of *do-it-yourself-biologists* has indeed got attention of the authorities. The American Federal Bureau of Investigation (FBI) “has adopted what some call a ‘neighbourhood watch’ stance. The approach relies on biohackers monitoring their own community and reporting behaviour they find threatening” (Ledford 2010). If indeed second hand tools for genome assembly are becoming available to the public at affordable costs then this would seem to add weight to the concerns over possible misuse of synthetic biology research (Balmer and Martin 2008).

Is there a relevant difference between dual use issues in ‘classic’ biology and in synthetic biology. Tucker and Zilinskas state that “the most likely misapplication of synthetic biology for hostile purposes involves the recreation of *known* pathogenic viruses in the laboratory” (Tucker and Zilinskas 2006, p. 16). If this is the case, the new element is in the aspect of *recreation* (e.g. of the Spanish flu virus). Problems can arise if such a recreated virus is misused for biological weapons or bioterrorism. But there is essentially no difference with the dual use issue in traditional biology. Although there still are many unknown factors Tucker and Zilinskas think it “likely that, given the difficulty of anticipating and assessing the risks associated with synthetic organisms, synthetic biology will require a new approach to regulation that differs significantly from the NIH [National Institutes of Health] Guidelines on recombinant DNA [Deoxyribonucleic acid]” (Tucker and Zilinskas 2006, p. 19). Already in 2006 the United States synthetic biology community proposed some measures that can be seen as an addendum of existing guidelines (Maurer et al. 2006):

- Insist That All Commercial Gene Synthesis Houses Adopt Current Best Practice Screening Procedures.
- Create and Endorse New Watch-Lists To Improve Industry Screening Programs.
- Create a Confidential Hotline For Biosafety and Biosecurity Issues.
- Affirm Members' Ethical Obligation to Investigate and Report Dangerous Behavior.
- Create a Community-Wide Clearinghouse for Identifying and Tracking Potential Biosafety/Biosecurity Issues.
- Endorse Biosecurity/Biosafety Research&Development Priorities.

Most of these measures have a procedural character that is not specific for synthetic biology. These measures could be applied in a general biosecurity policy. In fact some of them are common practice already in a number of countries and laboratories. An important question regarding the possible dual use of synthetic biology is a rather pragmatic one: why take the long and complex way of synthesizing a biological weapon, if in practice there are many more and easier ways to reach the same result? This is confirmed by the American biologist Drew Endy. He estimates the risks for the short and medium term very low. "From a security perspective, many people are concerned that it is now possible to directly construct harmful pathogens from DNA sequence information. This seems to me a real but remote possibility, and is likely best addressed by improvements in our capacity to respond to emerging infectious diseases, natural or otherwise, and to our public health systems. The more pressing security concern is to ensure that the tools and policies defining the future of biotechnology do not directly or inadvertently lead to a remilitarization of biology by nations." (Endy 2010)

The example of the discussion on synthetic biology shows that attention for dual use has spread widely in the life sciences during the past decade. The example also makes clear that the emphasis in the discussion is placed more on the possible consequences of misusing synthetic biology (new diseases etc.) than on the question how (un)realistic such a threat is.

### **Dual Use Reconsidered: Consequences or Intentions?**

The discussion on synthetic biology confirms an assertion of Pustovit and Williams. They perceive two main approaches to dual use technology: the Anglo-American pragmatic approach and the continental metaphysical approach (Pustovit and Williams 2008). According to the authors these approaches are based on different understandings of technology: the Anglo-American approach "is associated with technology notion as a sequence of processes and operations aimed to products with necessary and *useful for people properties*. The second one with enough neutral definition-understanding of technology as use of organized knowledge for aiming at practical goals by systems of machines and people" (Pustovit and Williams 2008, p. 2). In their view the Anglo-American approach is directed at concrete technologies, the continental one also at the role and intentions of people. The authors illustrate the 'American' view by referring to the phrase "dual use research

of concern” that has been developed in the—already mentioned—famous Fink-report of the National Research Council of the National Academies (2004), the starting point and analytical fundament of the present biosecurity debate in the United States, and not only there. Dual Use Research of Concern is defined as “research that, based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be directly misapplied by others to pose a threat to public health and safety, agriculture, plants, animals, the environment, or material” (National Research Council of the National Academies 2004). The list of experiments of concern has now an almost official status. Experiments of concern are those that:

- Demonstrate how to render a vaccine ineffective;
- Confer resistance to therapeutically useful antibiotics or antiviral agents;
- Enhance the virulence of a pathogen or render a non-pathogen virulent;
- Increase the transmissibility of a pathogen;
- Alter the host range of a pathogen;
- Enable the invasion of diagnosis and/or detection by established methods;
- Enable the weaponization of a biological agent or toxin.

It is referred to in many other publications, such as the report that Miller and Selgelid wrote for the Australian government (2008). Miller and Selgelid add some other categories:

- Genetic sequencing of pathogens;
- Synthesis of pathogenic micro-organisms;
- Any experiment with variola virus (smallpox);
- Attempts to recover/revive past pathogens.

According to Pustovit and Williams in declaring activities or technologies as ‘dual use’, the emphasis is laid upon the *possible* consequences of applications of the technology as such. Indeed, it is not difficult to describe those consequences for all of the above ‘experiments of concern’. An example is altering the host range of a pathogen. If a pathogen can be changed in such a way that it can survive not only in e.g. animals, but also in human beings, this can lead to new diseases for mankind. Animal diseases become human diseases. And because antibiotics or other remedies for such new diseases do not (yet) exist, the consequences can be disastrous. The risk of the transfer of animal diseases to humans is not imaginary, as is shown by the bird flu and more recently in The Netherlands by the Q-fever that is transmitted to humans by pregnant goats and sheep.

However, a consequence of putting (too) much emphasis on possible consequences of (mis)use of life science technologies, could be that the aspect of threat or intention gets too less weight in declaring a technology as dual use. The assignment of the label “dual use” should not only be determined by the biological, chemical or physical properties of the technology as such, but also by realistic interpretations and expectations about the way the technology will be used. In other words: an artefact, a technology or a natural product will become “dual use” only by a combination of (technical) properties and intentions. Let us make the comparison

with the kitchen knife: only in very exceptional circumstances a knife becomes a weapon.

The question is if Pustovit and Williams are right in making this sharp distinction between an Anglo-American and a continental approach. The existing or perceived threats were the starting point for the Fink Committee. The Committee was charged “to consider ways to minimize threats from biological warfare and bioterrorism without hindering the progress of biotechnology, which is essential for the health of the nation” (National Research Council of the National Academies 2004, p. vii). Given the professional and scientific background of the Committee members it is fully understandable that they concentrated on the scientific and technical aspects of the problem and not on the political and security aspects. In fact, Miller and Selgelid’s approach also clearly emphasises both consequences and intentions. For example, they explicitly state: “For something to be an instance of a dual use dilemma both outcomes (the two horns of the dual use dilemma) need to be (actually or potentially) intended...” (Miller and Selgelid 2008, p. 12). So Pustovit and Williams’ presentation of a sharp dichotomy between the views expressed in the literature is somehow misleading. That said, it is important to make clear that both intentions and consequences are in play.

The relevance of identifying a threat for defining dual use is also the point of view of John Forge (2009): “to classify something as dual use should not simply be the flag that the item *could* have some bad use, that some bad use is in theory possible (...) for artefacts at least, there has to be some threat to make and use an improvised weapon for it to be dual use”. Furthermore Forge remarks that threats come and go. This means that a technology or an artefact that is labelled as dual use today does not have to be necessarily a dual use issue tomorrow. This is a very relevant remark, because it focuses attention on questions as: is there a threat?; what kind of a threat is it?; who determines if there is a threat?; is this threat serious enough to declare a technology or an artefact as dual use?; etc. Maybe the most important, but often neglected question is: when does a threat, and thus a dual use marking disappear and who is to decide this? Sometimes it seems that since the terrorist attacks and the anthrax letters of 2001 almost irreversible steps have been taken to counter a possible terrorist or—more specific—bioterrorist threat. Now, almost 10 years later the question could be raised if the events since 2001 still justify this focus on bioterrorism and biosecurity.

Before further elaborating on these questions, some remarks will be made on the relationship between threats and intentions. This will be done by introducing two translations of the word threat in Dutch: *dreiging* and *bedreiging*. They mark a difference that does not exist in the same way in English. *Bedreiging* is used if an actor is threatening to act in a certain way, e.g. with using violence. Threat as *bedreiging* looks at a situation from the perspective of the subject making a threat. *Dreiging* on the other hand focuses at the perspective of the person or group that is or feels threatened. The *dreiging* perspective of threat does not have to coincide with that of *bedreiging*. Someone can feel threatened while in fact there is no real threat, because no one has the intention to commit an action against this person. The reverse is also possible: someone does not feel threatened, while in fact a real threat exists, because an actor has the intention to commit a crime or a terrorist action.

There are indications that the aspect of *dreiging* is most influential in the recent debates on biosecurity. Because of that the chance exists that in declaring an activity as dual use an emphasis is laid on the dual use potentiality and that there is an underestimation of the aspect of intentionality (*bedreiging*).

Recent history seems to confirm this assertion. If we take a look at the examples of threats that are presented as illustrations (or perhaps even proofs) of the threat, it is remarkable that—even in the recent *National Strategy for Countering Biological Threats* of the United States(US) National Security Council (2009)—only three already well known examples and one suspicion are recorded. These examples are: the Rajneeshee attack with a contaminated salad in Oregon (1984); contamination with anthrax spores by Aum Shinrykio (Japan) and the anthrax letters in the US (2001). The suspicion that Al Qaida might be preparing a bioterrorist attack was found after the occupation of Afghanistan. Three examples in more than 25 years! Of course the seriousness of each of these examples should not be underestimated. But for politicians and for decision makers in the life sciences it should be a serious consideration if these cases really justify the whole range of measures that haven been taken during the past years. Judith Reppy summarizes the developments in life sciences of the past decade with the conclusion that “concerns about bioterrorism raise the issues of dual-use technology in a field that until recently was not of much interest to the military” (Reppy 2006, p. 7). These developments have lead to what is called a securitization of life sciences and of public health (Kelle 2005).<sup>4</sup>

## Securitization of Life Sciences

Securitization is a concept that has been developed in the 1990 s by the Danish political scientist Ole Wæver. Because of that securitization is seen as a concept of the Copenhagen School of International Relations. This school is closely related to the English School, represented by theorists as Barry Buzan (Buzan 2001). For Wæver security is a *speech act*. “It is by labeling something a security issue that it becomes one” (Wæver 2004, p. 13). Stating that a particular *referent object* is threatened in its existence claims a right to extraordinary measures to ensure the referent objects survival. The issue is then moved out of the sphere of normal politics into the realm of emergency politics, where it can be dealt with swiftly and without the normal (democratic) rules and regulations of policy making. For the content of security this means that it has no longer any given meaning but that it can be anything a securitizing actor says it is. Security—understood in this way—is a social construction, with the meaning of security dependent on what is done with it (Taureck 2006). “‘Security’ is the move that takes politics beyond the established rules of the game and frames the issue as a special kind of politics or as above politics. Securitization can thus be seen as a more extreme version of politicization. In theory, any public issue can be located on the spectrum ranging from nonpoliticized (...) through politicized (...), to securitized (...). This link between

<sup>4</sup> Alexander Kelle argues that the process of securitization in the life sciences already started in the 1990s.



politicization and securitization does not imply that securitization always goes through the state, politicization as well as securitization can be enacted in other for a as well” (Taureck 2006, p. 23–24). Securitization studies aim to understand “who securitizes, on what issues (threats), for whom (referent object), why, with what results, and not least, under what conditions” (Buzan et al. 1998, p. 32). Translated to the dual use issue the main questions are: (a) did a securitization process take place in the life sciences and (b) if so how did it influence the dual use issue?

According to Fidler and Gostin securitization of public health means “that the theory and practice of public health are increasingly considered in security terms” (Fidler and Gostin 2008, p. 121). This is a rather new development, not only in health care, but also in the broader world of the life sciences. Public health and life sciences on the one hand and security on the other hand were until a few years ago almost completely separated worlds. “Biologists and other life scientists were—unlike the physicists—not involved in security politics, except for a relatively limited group of biologists and other life scientists who were working in Defence laboratories in order to develop biological weapons or to contribute to biodefense research” (van der Bruggen 2009, p. 69). But most of these life scientists did not take part in public debates on biological weapons or—broader—weapons of mass destruction, like e.g. physicists did on nuclear weapons.<sup>5</sup> This has changed in the past decade. The following reasons can be distinguished for the securitization of the life sciences (Van der Bruggen 2009).

A first reason for securitization is the reference to the events of 11 September 2001 and the anthrax letters in the same period. Undoubtedly these events were an important reason for seriously considering if life sciences could be a source for terrorist attacks. But some qualification has to be considered. First of all: the anthrax attack was the result of the actions of one deranged researcher who was working in a Defence laboratory. He had no link with any terrorist or radicalized (Muslim) organization. This makes his deeds no less repugnant, but this fact should have influenced the threat analysis. Of course it has taken some years before this conclusion could be drawn definitively, but from the beginning the experts knew that the anthrax spore came from one of the American Defence laboratories. Nevertheless it is a legitimate question to investigate the risks of a comparable threat by terrorist groups. But how credible is it to expect a bioterrorist threat from these groups? Are there really any indications for such an expectation? Of course intelligence services will have to perform their inquiries. And it is understandable that they do not make all their results public. So it cannot be excluded that there really are some indications for a threat.

A second reason for securitization can be found in the initiatives of the BTWC State Parties during the 5th and 6th review conferences and the intersessional meetings to stimulate awareness raising among scientists, e.g. by developing codes of conduct. Attention—also within BTWC—shifted from state actors to non state actors and the risks of bioterrorism. And, of course, most of these discussions were held in the same time that the world was confronted with a series of terrorist attacks.

---

<sup>5</sup> A well-known example of the involvement of physicists is the Pugwash Conference, which was initiated by concerned scientists as Albert Einstein. See: [www.pugwash.org](http://www.pugwash.org).

This gave an extra argument to involve the scientific world in the BTWC activities (Revill and Dando 2009).

A next important reason is the occurrence of (new) infectious diseases that threaten humans as well as animals: Acquired Immune Deficiency Syndrome (AIDS), Severe Acute Respiratory Syndrome (SARS) and the Bird Flu are the most well-known examples. Some authors—as Fidler and Gostin—put naturally occurring infectious diseases under the heading of biosecurity (Fidler and Gostin 2008, p. 2). They see this broadening of the security concept as an effort to release the concept of security from the “traditional state centred military-biased perspective” (Fidler and Gostin 2008, p. 6). In their opinion public health and security are unjustly two almost completely separated worlds. They refer to the concept of human security to defend their view (Human Security Centre 2005). Although there are divergent interpretations of human security, a common denominator is that the concept of security should be broader than national or military security. All proponents agree that the primary goal of human security is the protection of human individuals. This broadening of the concept of security implies that there should not only be attention for prevention of possible threats of intentional spreading diseases. Security issues are also at stake because of the effects of diseases, irrespective if these are intentionally causes or not. Pandemic explosions can lead to societal unrest and even upheavals.

Globalization has in at least two ways led to more attention for biosecurity issues. First, a growing number of international personal and commercial contacts may contribute to a faster and more extensive spread of viruses around the world. Local epidemics can become national or even global epidemics. There are examples of sources for diseases (such as the malaria mosquito) that are spread to new regions (e.g. because of climatic changes or as a ‘stowaway’ in a plane or ship). Globalization also promotes the international contacts between scientists and researchers. Personal exchange, appointments abroad and international conferences have grown exponentially during the past decades. The advantages of this development are obvious. Science and technology flourish because of it. More people from more countries are able to contribute to science. But there is the other side that intentional or unintentional misuse is made of scientific results. In The Netherlands the example of the Pakistani nuclear scientist Dr. Khan is well known. He was from May 1972 to December 1975 working at an engineering firm based in Amsterdam and a subcontractor to the Uranium Enrichment Corporation (URENCO) specializing in the manufacture of nuclear equipment. URENCO’s primary enrichment facility was at Almelo, Netherlands. A. Q. Khan, in his capacity would eventually have an office at that facility by late 1974. In early 1976, Dr. Khan left the Netherlands with secret URENCO blueprints for a uranium centrifuge.

Last but not least another consequence of globalization is that terrorist activities are no longer limited to regional and local conflicts. Unlike the Irish Republican Army (IRA) or Euskadi Ta Askatasuna (ETA), groups as Al Qaeda have made the entire world to their working area.

The preceding paragraphs provide answers to the questions that were formulated above: (a) did a securitization process take place in the life sciences and (b) if so how did it influence the dual use issue? There has to be no doubt that indeed a process of securitization has taken place in the life sciences. The main actors of this

securitization process are politicians and policy makers as well as the scientific community itself. The main reasons are political (9/11; BTWC, globalization) as well as scientific (new epidemics, scientific developments). In relation to the second question it can be established that due to this securitization process dual use has become an issue for the life sciences. The publication of the Fink report in 2004 is a first milestone in this development. A great range of national and international activities have taken place since then, varying from expert meetings of the BTWC to national codes of conduct and education and training courses.

### **Securitization and Dual Use Policy: Some Caveats**

Taking all these developments into account, the question remains if the biosecurity risk indeed is significantly greater than 10 or 25 years ago. Can the securitization process be declared and justified. Is it really necessary to mobilise the life sciences community and make them aware, or are we pulled along in a whirlpool of developments that have led to an overexposure of perhaps not or hardly existing biosecurity risks? It is not easy to give a validated answer to this question, if only because there is much confidential information held by intelligence services and other government officials on the occurrence of incidents. Moreover it is hard to prove that or why some incidents have *not* happened. Comparable discussions took place on the effectiveness of nuclear deterrence during the Cold War: it cannot be proven that nuclear deterrence really has prevented the occurrence of (nuclear) war. But did a nuclear war not occur because of the effectiveness of nuclear deterrence or maybe because there was no real threat?

Can the same be said of dual use policy for the life sciences? Some caveats are in place.

The first caveat is about the reaction of the state and that of the public to the terrorist threat. When after September 2001 the threat of a terrorist attack moved up the chart of security risks, it was clear from the beginning that government saw a prominent role for itself in reducing that threat. This is understandable because terrorism belongs to the kinds of threats that are directed against the state as such, which is not the case with e.g. airplane crashes. This link with the 'core business' of government led to a revival of the role of the state as the ultimate guardian of security. Shortly after September 11 Francis Fukuyama (one of the prophets of neo-liberalism) wrote very strikingly that it is not the Microsofts of this world that send aircraft carriers (Fukuyama 2001). Therefore a state with its monopoly of violence is necessary! The new security issues made clear that there are domains where public and political responsibilities come first. In the years after 9–11 governments took up numerous activities and institutions to reduce terrorist threats. In general these activities were supported by the population, even if it led to measures that could be seen as limitations of individual freedom or privacy. This acceptance can be related to a high level of subjective insecurity. Many people feared new terrorist attacks.

But how does this subjective (feeling of) insecurity (*dreiging*) relate to the objective level of insecurity that is caused by potential bioterrorism (*bedreiging*)? Certainly the risk of dying because of a bioterrorist attack is many times smaller

than the chance of dying in a traffic accident. But the social shock and distress are much greater. This can be explained by the fact that terrorist attacks hit society as such. If 3,000 people would have been killed after the World Trade Centre had fallen down because of an earthquake, the shock would have been great also, but incomparable with what happened after 9–11. The essence of the state and the capability of the state to protect its citizens were at stake! The terrorist attack was seen as an act of war, comparable with the attack on Pearl Harbour in 1941. This view explains the reaction of governments, not only in the United States, but also in many other states. The reactions to 9/11 clearly show that governments are willing to spend more financial and personal means to counter terrorist threats than other security risks, which do not directly affect its core tasks.

Another phenomenon that can be observed is the tendency of policy makers to think in worst case analyses rather than in probabilities. Again a plausible explanation can be given. Our views and images of terrorism have been formed by the attack on the World Trade Centre and the massive attacks in Madrid and London. For these kinds of terrorist attacks even a new name has been created, catastrophic terrorism: attacks using weapons of mass destruction or more simple methods to kill thousands of civilians for political pressure, political theatre, or crazed self-expression (Fearon 2003). Although political authorities are aware of the low probability of terrorist attacks they are prepared for the worst: policy is developed that is based on such worst case scenarios.

A third caveat has a more psychological character: a phenomenon that can be identified as anticipated decision regret. Anticipated decision regret is an attitude of people which leads them to take actions that are directed at preventing possible future incidents. If I take this preventive measure now, it will mean that I do not have to blame myself (or get blamed by others) for not having done everything to prevent that incident from happening. This attitude also can be observed in health care. A growing number of preventive screening tests are offered that provide information of the chance of developing some kind of disease. It is often not taken in consideration that the chance of really getting this disease is very small. And it is possible that the measures that are taken to prevent the disease negatively influence lifestyles. The Dutch medical sociologist Tjeerd Tijmstra (2001) gives some—often hilarious—examples of anticipated decision regret: if a mother gets a screening test for her child offered for a disease for which the risk is 1 in 90,000, there is a great willingness to participate. And even if it is explained to people that the chance of having a car accident while driving to the clinic is about as much as that particular risk, still many people decide to go on. Their motivation seems to be: suppose our baby does develop that disease, then we should not forgive ourselves not to have done everything to prevent it. There are signals that this anticipated decision regret has become an attitude in security issues also. But in the field of security governments and other public agencies (such as scientific organizations) are bearers of the attitude more than individual citizens. After 9/11—let it be repeated again—security measures against possible terrorist attacks have been given an enormous priority. It looks as if governments are willing to invest a lot of energy in minimizing the chances of terrorist attacks. They do not want to take the risk that they have not done everything to prevent an assault. This attitude can be based on

experience. Officials of the Dutch government were reproached for not having done enough to prevent the murder of film director Theo van Gogh (2004). These reproaches have led to decisions that are directed at minimizing the chance of new attacks. With—in general—societal and political support a good deal of money and a lot of energy are devoted to this topic. It is not farfetched to suppose that this is one of the effects of our common anticipated decision regret.

### **Dual Use Policy in the Life Sciences Reconsidered: Proposal for a Definition**

The considerations that have been presented in the previous pages might the reader lead to the assumption that there is no much need to worry about bioterrorism and that most measures are highly exaggerated. That would not be a right assumption. There are reasons to be cautious for the risks of bioterrorism. But one should not stop thinking! Anti terrorist policy should not be carried out on autopilot. Fortunately, many politicians and officials of the Intelligence services are among the first ones to stress that possible acts of Chemical, Biological, Radiological or Nuclear terrorism (CBRN) do almost certainly not imply the use of weapons of mass destruction with thousands of victims, but of less destructive (although of course still very dangerous and harmful) weapons.

But still it is possible that politicians and officials are so much preoccupied with anti-terrorism policy that all information is interpreted in such a way that it strengthens the conviction that already exists. In that case information that contradicts this conviction or that is not directly relevant could be underestimated or neglected. A focus on security issues can lead to an attitude where other policy issues are subordinated to security issues or will be judged only in their relation to security issues. To give a fictitious, but not unrealistic example from the life sciences: why is a student from a Middle East country coming to this European laboratory for his PhD research? The idea that this person just wants to become a good scientist in order to help his country in fighting serious diseases could be set aside by the bias driven view that he or she could be a potential terrorist, so “we will watch him and prevent him from stealing materials”.

This example brings us back to the dual use policy as it has been developed in the past years. The conclusion is that there is nothing wrong with more awareness of the potential dual use that can be made with the materials or the results of life sciences research, but this awareness should not become so predominant that distrust is the default attitude in a laboratory. Codes of conduct, like the Dutch Code of conduct for biosecurity have proven to be an appropriate method to make life scientists and other people that are involved in biotechnological research aware of the dual use issue without exaggerating the risks (Koninklijke Nederlandse Akademie van Wetenschappen 2009).

In almost all discussions that were entered in relation to the Code of Conduct a conclusion was that such a Code alone is not enough to limit the risk of the misuse of dual use technology. Measures have to be taken to reduce the risk of dual use research and technology beyond the spheres of awareness. It will be important to go

on with this policy on the basis of cooperation between all involved parties: scientists, funding organisations, universities, hospitals, politicians, officials of ministries and of course experts on terrorism and anti-terrorism. Such cooperation does not only take away possible misunderstandings, but it is also an appropriate remedy against possible tunnel visions, that could lead to an overemphasis of biosecurity. Although it is very useful to pay attention to possible developments in an early stage, possible dual use should not get such a high priority that promising developments in e.g. the field of synthetic biology are hampered or that talented researchers from abroad (especially from suspected countries) do not get the chance to participate in research.

At the end of this article, I translate the main conclusions into a proposal for an acceptable, adequate and applicable definition of the dual use concept for researchers, universities, companies and policy makers. The reason for proposing such a new definition is not academic in nature. The intention is to offer a definition that will be consistent with existing definitions of dual use, but wider. The conclusion of the above cannot be otherwise than that a definition of dual use should encompass more than only the technical or physical properties of a biological agent. Dual use policy should be based upon a deliberate consideration of technical possibilities, threats and intentions and possible consequences.

The most common and authoritative definition still is the earlier mentioned one in the Fink-report (National Research Council of the National Academies 2004): Dual Use Research of Concern is: “Research that, based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be directly misapplied by others to pose a threat to public health and safety, agriculture, plants, animals, the environment, or material”. The definition is explained by the list of seven experiments of concern. In a recent publication Selgelid (2009) proposes three plausible definitions of dual use science and technology:

- That which has both civilian and military applications;
- That which can be used for both beneficial/good and harmful/bad purposes, and
- That which has both beneficial/good and harmful/bad purposes—where the harmful/bad purposes involve weapons, and usually weapons of mass destruction.

As the authors of the Fink report and Selgelid are aware, uncertainties are inherent to both threats and expected damage. Moreover, as argued above, both intentions and consequences need to be involved in defining dual use. Further, too much emphasis on worst case scenarios is problematic. These kinds of scenarios describe the disasters that (can) take place if indeed the biological agent is misused for terrorist or criminal intentions. But worst cases are not by definition realistic scenarios. Because of that a definition of dual use should not only be based on elements that point to worst cases. So—with all necessary restraint—this definition will be proposed:

A dual use problem arises when

1. research, based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be misapplied and;

2. there is a recognizable threat and a not negligible chance of such misuse and;
3. there are serious consequences for society and science (public health and safety, agriculture, plants, animals, the environment, or material).

**Acknowledgments** I express my thanks to prof. Dr. Seumas Miller, Dr. Michael Selgelid, the members of the valorisation panel of the project *Biosecurity & Dual Use Research* of the Dutch Research Council (NWO) and two anonymous reviewers for their valuable remarks and comments to earlier drafts of the manuscript.

**Open Access** This article is distributed under the terms of the Creative Commons Attribution Non-commercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

## References

- Balmer, A., & Martin, P. (2008). *Synthetic biology, social and ethical challenges*. Nottingham: Institute for Science and Society, University of Nottingham.
- BTWC. (2006). Final document of sixth review conference of the states parties to the convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction, BTWC, Geneva.
- BTWC. (2008). *Document BWC/MSP/2008/L.1*. Geneva: BTWC.
- Buzan, Barry. (2001). The English school: An underexploited resource in IR. *Review of International Studies*, 27(3), 471–488.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner Publishers.
- Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction. (1972). London, Washington, Moscow.
- de Vriend, H. (2006). *Constructing life. Early reflections on the emerging field of synthetic biology*. The Hague: Rathenau Institute.
- Endy, D. (2010). Testimony to the house committee on energy and commerce on advances in synthetic biology and their potential impact. Washington, DC, 27 May 2010. Retrieved January 3, 2011, zie <http://energycommerce.house.gov/documents/20100527/Endy.Testimony.05.27.2010.pdf>.
- Fearon, J. D. (2003). *Catastrophic terrorism and civil liberties in the short and long run*. Stanford: Department of Political Science, Stanford University, 10/9/03. Accessed October 14, 2010, from [www.stanford.edu/~jfearon/papers/civlibs.doc](http://www.stanford.edu/~jfearon/papers/civlibs.doc).
- Fidler, D. P., & Gostin, L. O. (2008). *Biosecurity in the global age, biological weapons, public health and the rule of law*. Stanford: Stanford University Press.
- Forge, J. (2009). A note on the definition of ‘dual use’. *Science and Engineering Ethics*. Published on line August 14, 2009, doi:10.1007/s11948-009-9159-9.
- Fukuyama, F. (2001). Amerika moet een gewoon land worden. *NRC Handelsblad*, 18 September 2001 (Translation from article in *Financial Times*).
- Human Security Centre. (2005). *The human security report 2005. War and peace in the 21st century*. New York—Oxford: Oxford University Press.
- International Atomic Energy Agency (IAEA). (2006). *Medium term strategy 2006–2011*. Accessed October 14, 2010 from [http://www.iaea.org/About/mts2006\\_2011.pdf](http://www.iaea.org/About/mts2006_2011.pdf).
- Kelle, A. (2005). *Bioterrorism and the securitization of public health in the United States of America—Implications for public health and biological weapons arms control*. Bradford regime review paper no. 2, Bradford: Bradford University.
- Koninklijke Nederlandse Akademie van Wetenschappen. (2009). *Eindverslag van de Werkgroep Biosecurity*. Amsterdam: KNAW.
- Ledford, H. (2010). Life hackers. *Nature*, 467, 650–652.
- Maurer, S. M., Lucas, K. V., & Terrell, S. (2006). *From understanding to action, community-based options for improving safety and security in synthetic biology*. Berkeley: University of California.

- Miller, S., & Selgelid, M. J. (2008). *Ethical and philosophical consideration of the dual-use dilemma in the biological sciences*. Dordrecht: Springer.
- National Research Council of the National Academies. (2004). *Biotechnology research in an age of terrorism* ["The Fink Report"]. Washington DC: NRC.
- National Security Council. (2009). *National strategy for countering biological threats*. Washington DC: NSC.
- Pustovit, S. V., & Williams, E. D. (2008). Philosophical aspects of dual use technologies. *Science and Engineering Ethics*. (on line 21 October 2008), <http://www.springerlink.com/content/w48w717k0313481v/?p=f22509445ae84158ba20343b66c9d855&pi=3>.
- Reppy, J. (2006). Managing dual-use technology in an age of uncertainty. *The Forum*, 4(1), Article 2, 1–10.
- Revill, J., & Dando, M. (2009). The rise of biosecurity in international arms control. In B. Rappert & C. Gould (Eds.), *Biosecurity: Origins, transformations and practices* (pp. 41–59). Basingstoke: Palgrave Mac Millan.
- Selgelid, M. (2009). Dual-use research codes of conduct: Lessons from the life sciences. *Nanoethics*, 3, 175–183.
- Taureck, R. (2006). *Securitisation theory—The story so far: Theoretical inheritance and what it means to be a post-structural realist*. Paper for presentation at the at the 4th annual CEEISA convention. University of Tartu, 25–27 June 2006.
- Tijmstra, T. (2001). Het imperatieve karakter van medische technologie en de betekenis van 'geanticipeerde beslissingsspijt'. In Marc Berg en Annemarie Mol (Ed.), *Ingebouwde normen. Medische technieken doorgelicht* (pp. 40–45). Utrecht: van der Wees.
- Tucker, J. B., & Zilinskas R. A. (2006). The promise and perils of synthetic biology. *The New Atlantis*, March 2006. Accessed October 14, 2010 from <http://www.synbiosafe.eu/uploads/pdf/The%20Promise%20and%20Perils%20of%20Synthetic%20Biology.pdf>.
- van Andel, P. (1994). Anatomy of the unsought finding: Serendipity: origin, history, domains, traditions, appearances, patterns and programmability. *British Journal for the Philosophy of Science*, 45(2), 631–648.
- van der Bruggen, K. (2009). Science of mass destruction: How biosecurity became an issue for academics of science. In B. Rappert & C. Gould (Eds.), *Biosecurity: Origins, transformations and practices* (pp. 60–78). Basingstoke: Palgrave Mac Millan.
- Wæver, O. (2004). *Aberystwyth, Paris, Copenhagen new schools in security theory and the origins between core and periphery*. Paper presented at the ISA Conference Montreal, 2004.