Sci Eng Ethics (2013) 19:461–486
DOI 10.1007/s11948-012-9357-8

ORIGINAL PAPER

The Just War Theory and the Ethical Governance of Research

Ineke Malsch

Received: 22 September 2011 / Accepted: 13 February 2012 / Published online: 28 February 2012

Abstract This article analyses current trends in and future expectations of nanotechnology and other key enabling technologies for security as well as dual use nanotechnology from the perspective of the ethical Just War Theory (JWT), interpreted as an instrument to increase the threshold for using armed force for solving conflicts. The aim is to investigate the relevance of the JWT to the ethical governance of research. The analysis gives rise to the following results. From the perspective of the JWT, military research should be evaluated with different criteria than research for civil or civil security applications. From a technological perspective, the boundaries between technologies for civil and military applications are fuzzy. Therefore the JWT offers theoretical grounds for making clear distinctions between research for military, civil security and other applications that are not obvious from a purely technological perspective. Different actors bear responsibility for development of the technology than for resorting to armed force for solving conflicts or for use of weapons and military technologies in combat. Different criteria should be used for moral judgment of decisions made by each type of actor in each context. In addition to evaluation of potential consequences of future use of the weapons or military technologies under development, the JWT also prescribes ethical evaluation of the inherent intent and other foreseeable consequences of the development itself of new military technologies.

Keywords Just War Theory · Research ethics · Nanotechnology · Emerging technology · Governance

I. Malsch (✉)
Malsch TechnoValuation, Vondellaan 90, 3521 GH Utrecht, The Netherlands
e-mail: postbus@malsch.demon.nl
URL: www.malsch.demon.nl

Introduction

This article contributes to the current debate on the governance of key enabling technologies such as nanotechnology. In this debate, the implications of nanotechnology and converging technologies for security have so far received relatively little attention from policymakers, stakeholders, ethicists and social scientists.

This article does not presuppose the categorical distinctions between research and development. This is because in emerging sciences and technologies such as nanotechnology and converging technologies, traditional engineering characteristics including interdisciplinary cooperation on common problems on the boundary between scientific disciplines are introduced in the earlier stages of research. This trend has been ongoing at least since the 1990s. The distinction has also become less pronounced due to the changing roles of industry and academia in research and development, where academic research has become increasingly applied and there is more interest in open innovation in the triple helix of academia, industry and governments. The move from basic to application-oriented to applied research has become more fluid and traditional boundaries have become less important (e.g. Leydesdorff and Etzkowitz 1996).

Furthermore, the distinction between science and technology and products, equipment, or weapons is becoming increasingly blurred because of trends in dual-use sciences and technologies that are ever-cheaper and more easily available for military and terrorist uses (c.f. synthetic biology, amateur life sciences facilitated through the availability of cheap equipment for life science research and easier access to scientific research results through the internet).

The last decade has witnessed an extensive stakeholder debate and analysis by ethicists and social scientists on many ethical or social aspects of nanotechnology. This high level of attention for the societal implications of technology in a relatively early stage of development has been inspired by the desire of policymakers to prevent public controversy after its large scale market introduction. This happened in the case of Genetically Modified Food in Europe. Policymakers were in a position to invest in research into ethical and social aspects because in the early 2000s, most of the funding for nanotechnology came from public sources. To avoid such a controversy over nanotechnology, national governments and the EU have invested a substantial amount of money into projects that investigate the ethical, legal and social aspects of nanotechnology (nanoethics and ELSA) and into public and stakeholder dialogues.[1] Nanotechnology has so far not given rise to the identification of new ethical issues. Still, the same ongoing discussions about the ethical aspects of technological systems and products where nanotechnology can be applied are also relevant to nanotechnology for those applications.

On the other hand, security related nanotechnology has received relatively little attention from policymakers, stakeholders, ethicists and social scientists. There are however a few notable exceptions: Altmann (2005, 2006, 2008), Gsponer (2007), Gubrud (1997), van den Hoven and Vermaas (2007), Nasu and Faunce (2009), and Schummer (2001). Most of the authors who discuss governance and the ethical

[1] Risk assessment projects have also been funded on the basis of the constitutional government's responsibilities for occupational health and safety, environment and public health.

aspects of security technologies or dual-use science and technology apparently do not see the relevance for their subject of the emergence of nanotechnology. Conversely, most authors who discuss governance and the ethics of nanotechnology tend not to pay attention to security related aspects because the debate is often conducted along the axis of economic benefits versus the safety of individuals. The scientists, industrialists and policymakers who engage in the responsible development of nanotechnology with security implications need more information about ethical issues related to security technologies. The governance of nanotechnology for those applications should be inspired by the relevant ethical theories.

In this article, nanotechnology developments are analyzed from the perspective of the Just War Theory (JWT). Following Grotius, this is a current political philosophical theory concerning the correct conduct of international relations between states, based on an ancient theory of war and peace. (c.f. discussion in Nussbaum 2006, pp. 44–45) Historically, varying interpretations of the JWT have been applied by both governments and the peace movement. From the perspective of the peace movement, it is intended to make the threshold for going to war as high as possible and to make warfare practices as humane as possible. Despite the name, for peace activists the Just War Theory is ultimately aimed at fostering a more Just Peace. From the perspective of governments of sovereign states, the JWT is an ethical theory of the legitimate use of force. The relevance of the JWT to the ethical governance of a key-enabling technology like nanotechnology, which is applicable in multiple sectors including military and civil security, is investigated below. The relevance of the JWT is influenced by distinctions between different application domains (military, civil security and other) and between a philosophical-ethical and a technological approach to the discussion. Furthermore, the details of the parties and institutions that participate in security-related nanotechnology development and applications and the issues they are concerned with are needed to examine what the JWT can and cannot contribute to the discussion. Section "Relevance of the JWT to the development of technology" takes the ethical Just War Theory as a starting point and develops it into an instrument for evaluating decision making—by parties who are attributed responsibility from a theoretical perspective—on different types of technology development with implications for security. Section "Examining relevant contexts in actual practice" provides an overview of the actors who play a role in the real life of technological developments in nanotechnology and of current issues under debate in Europe. Section "Contributions of the JWT to the discussion" discusses what the Just War Theory can contribute to the current debate. In particular, it explores the question of to what extent taking the perspective of the JWT can give arguments why it would be good to restore traditional demarcations between research and technological development.

Relevance of the JWT to the Development of Technology

Just War Theory sets norms for the decisions of sovereign states that have the authority to decide on the appropriate response to external threats to their national and citizens' security. The philosophical JWT does not address the development of new weapons or other military technologies. For a thorough analysis of the Just War Theory, see Walzer

(1977). However, from a legal perspective, the JWT has been articulated in International Humanitarian Law, including the Geneva Conventions. Since 8 June 1977, Article 36 of the First Protocol of the Geneva Convention stipulated that "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."[2] This emphasis on future employment appears to limit the assessment of the development of military technology to the Jus in Bello criteria proportionality and discrimination through their elaboration in International Humanitarian Law. The Protocol does not consider other ethical aspects of the development of technology that would be problematic from a more comprehensive but not legally enforceable ethical JWT perspective. Would a broader consideration of the JWT as an ethical theory be relevant to the development of technology?

Traditionally, the JWT consists of two parts: Jus ad Bellum and Jus in Bello. Jus ad Bellum gives guidance to states that are preparing to go to war. It promotes review and raises the threshold for going to war. It is articulated in the following six cumulative criteria for a just war:

- Is the use of military force aimed at a just cause?
- Is it being deployed with a just intent?
- Does the party that decides about going to war have legitimate authority?
- Is going to war a proportional answer to the wrong to be avoided?
- Does the use of military means have a reasonable prospect of success?
- Is it the last resort?

From an ethical perspective, Jus in Bello attributes moral responsibility to military forces and soldiers, whether or not they are obliged to take such responsibility under national legislation. Jus in Bello is intended to minimize suffering during a war. It consists of two criteria that give guidance for the ethical behaviour of military forces: Discrimination/non-combatant immunity means that combatants may not intentionally harm civilians or soldiers that do not engage in combat (e.g. because they are wounded or have surrendered). Military proportionality means that the use of force should be proportional to the military ends sought.

The ethical principles of Jus in Bello have a legal counterpart in International Humanitarian Law; in particular the Geneva Conventions. International Humanitarian Law imposes enforceable rules on the conduct of warfare by states that have the legitimate authority to do so, in particular in Articles 35–38 of the First Protocol to the Geneva Convention. As international customary law, this also binds states that are not parties to the conventions.

Lietzau believes that contemporary international terrorism and the threat of WMD has given rise to changing interpretations of the JWT, in particular the Jus ad Bellum criteria. What constitutes legitimate preventive self-defence or illegitimate retaliation is open for discussion.[3] Another issue is whether the legitimate use of

[2] http://www.icrc.org/ihl.nsf/WebART/470-750045?OpenDocument.

[3] This view is contested. To many international lawyers, legitimate preventive self-defence is a contradictio in terminis, even those that like Grotius accept humanitarian intervention.

armed force is limited to self-defence or if humanitarian intervention should also be allowed (Lietzau 2004). Greenwood discusses developments in international humanitarian law (IHL) on weaponry and points out that five general principles are commonly used to assess the legality of weapons, including new types of weaponry: unnecessary suffering, discrimination, proportionality, prohibition of perfidy and to a lesser extent environmental protection. Since the 1990s, the realm of IHL has been extended to internal conflicts, in addition to its traditional international operational domain (Greenwood 1998). Likewise, Lawand discusses the legality of weapons and the means and methods of warfare under International Humanitarian Law (Lawand 2006). These and other authors argue from the perspective of the legal counterpart to the Just War Theory and emphasise the formal obligations of states that may or may not be party to relevant international treaties. This article discusses a complementary ethical interpretation of the JWT.

Some authors have applied the JWT to the use of specific military technologies in combat, e.g. to nuclear and biological weapons (O'Donovan 2003) and precision weapons (Schmitt 2005). These authors have applied the Jus in Bello criteria discrimination/non-combatant immunity and military proportionality most often in the traditional way: to morally evaluate the actions of the military command and the soldiers who use the weapons. They have not systematically applied the Jus in Bello criteria in the ethical evaluation of the contributions of those engaged in developing new weapons and other military technologies. In a discussion about challenges to the JWT posed by technological developments, O'Donovan (2003) argues that "the search for new and ever more effective weapon technologies encourages cruelty of mind." "Weapons technology has terrorised the twentieth century by running ahead of moral, political and legal control […] the practical question is always how to bring it under control. […] Prohibitions are unhelpful, unless accompanied by a serious attempt to apply moral reasoning to the task of weapons design."

From an ethical perspective, the JWT constitutes a framework for applying moral reasoning to warfare (broader than formal legal obligations of states); therefore this could also constitute a good foundation for considering the ethics of weapons design. Two aspects should be taken into account in applying ethical JWT to weapons design:

(a) Different actors in distinct contexts need different criteria to ethically evaluate or guide their actions
(b) The same research and technology may have both civil and military uses in the future

Firstly, traditional ethical JWT consists of two parts, each evaluating or guiding the actions of actors with different professional roles: governments of sovereign states and military forces. The criteria that are used to evaluate these actions are adapted to the context and responsibilities of the distinct groups. Since those involved in decisions on weapons design are also different actors operating in a different context, a targeted set of criteria must be proposed. These criteria could be similar to existing or different JWT criteria. For example, like all concepts of justice, Jus ad Bellum and Jus in Bello require the criterion of "proportionality", albeit adapted to the particular context. Proportional is not an exact measure to compare the magnitude of the intended use of force to the magnitude of the assault, but a moral concept for determining in advance or judging with hindsight whether or not a particular action can be deemed justifiable given what was known about the threat that was faced. The other criteria are different.

Secondly, there is no categorical demarcation between the development of research and technology for military and for civil uses. The intended use of a technology is increasingly articulated as the technology matures. The Defence Technology Readiness Levels (TRLs) range from 1 to 9. Level 1 is basic research and level 9 is the actual system proven through successful mission operation. Beginning at the prototype stage (TRL 6–7), its military uses are clearly distinguishable from other applications.[4] The same research and technologies at less advanced TRL that will in the future be essential for new products intended to save lives or improve the quality of life could be misused in weapons. Examples are nanobiotechnology and synthetic biology for use in pharmaceuticals and medical diagnostics.

The lack of a clear boundary between research and technologies for civil and security applications could call for a broad concept of moral weapons design. Whether an additional chapter of the JWT covering technological developments can be limited to actors responsible for decisions on priorities in military technology development (TRL 6–7 and higher) is still a matter under investigation. It might be necessary to extend these considerations to include those deciding on more basic research and on applied technology development for civil security and non-security related sectors. Even technologies that were not originally intended for military applications have a significant and increasing chance of eventually contributing to new weapons that escape moral, political or legal control. It is precisely the property of such technologies that prompted O'Donovan (2003) to call for moral weapons design.

Ethical JWT is designed to promote a review of matters of war and peace and to raise the threshold for the use of armed force. Malsch (2011) includes a bottom-up analysis of the applicability of individual Jus ad Bellum criteria to nanotechnology development. The analysis in the present article is top-down, taking the purpose of the JWT as the starting point. The following questions will be answered:

- What is the purpose of the JWT and which aspects make it useful for evaluating military technological development? (in Sect. "Purpose of the JWT")
- Who could be given the authority to make decisions regarding the development of new technologies? (in Sect. "Attributing responsibility for decision making")
- Which criteria included in the JWT or other ethical criteria appear relevant to make such decisions contribute to global peace and justice? (in Sect. "Characterising ethical decisions").

Purpose of the JWT

Ethical JWT is a special case of the theory of double effect. The theory of double effect investigates under which circumstances actions that cause evil effects as a side effect can be tolerated (Wils 2007). The theory includes four limiting principles:

[4] See also http://www.homelandsecurity.org/hsireports/DHS_ST_RL_Calculator_report20091020.pdf.

1. “that the action in itself from its very object be good or at least indifferent;
2. that the good effect and not the evil effect be intended;
3. that the good effect be not produced by means of the evil effect;
4. that there be a proportionately grave reason for permitting the evil effect” (Mangan 1949, p. 43 cited in McIntyre 2011).

The purpose of the theory of double effect is therefore to promote review and motivate ethical judgement about the intrinsic moral value of actions and about their potential future consequences. It condemns actions that are evil at the core and aims to avoid evil consequences as much as possible, while encouraging action undertaken with good intentions. A core question is of course what should be considered evil effects, as distinct from mere harmful effects. In the case of the Just War Theory, the evil effects in question include large-scale of suffering of people and massive destruction of the infrastructure and organisation of a territory. This is of a different order of magnitude than for example harm caused by the introduction into the market of an unsafe product or misuse of an item such as a kitchen knife to kill a fellow citizen. What should be considered the threshold beyond which harmful effects become evil is a matter open for debate. However, the theory of double effect presents a balancing framework that could also be useful for guidelines to determine whether or not actions with intended good and unintended foreseeable less severe but still bad effects could be justifiable. In such more mundane cases, good can be considered to mean contributing to a societal need and bad can be considered harming individual human rights, society or the environment on a modest scale.

In general, philosophical ethics makes a distinction between consequentialist and deontological theories. Consequentialist ethical theories evaluate actions by the effects they have, disregarding the intentions or behaviour of the actor. Deontological ethical theories on the other hand imply a concept of “duty” in that one was bound by the teachings of the ancestors in the obligations and responsibilities of being within the confines of a society. Interestingly, the theory of double effect in general—and the classical JWT in particular—combine consequentialist and deontological criteria. These theories are therefore more demanding than either general type of ethical theory alone. The deontological criteria of the JWT are just cause, just intent, legitimate authority and discrimination/non-combatant immunity. The consequentialist criteria are a reasonable prospect of success, proportionality and last resort. All the criteria must be fulfilled for a war to be considered just.

An expanded JWT that covers activities aiming at weapons design and military technology development should also set both deontological and consequentialist standards because these actions are undertaken in preparation for the use of force in international conflicts. Therefore they are expected to contribute to the same evil effects as decisions to go to war and actions of armed forces during a war. The purpose of the JWT from an ethical perspective could therefore make it extendable to military technology development and weapons design. As demonstrated above, a similar broadening of related International Humanitarian Law to the use and development of weapons has already been common practice for decades.

Attributing Responsibility for Decision Making

As noted, in classical ethical JWT two types of actors are attributed responsibility for making decisions under Jus ad Bellum and under Jus in Bello. Governments of sovereign states have the authority to make decisions on engaging in warfare and hence the responsibility to take ethically sound decisions. In addition to the legal responsibilities of states, military forces have a moral responsibility for the decisions made on the battlefield during war. The moral responsibility is more fundamental than and independent of any legal obligations in national law that make the misconduct of military forces and individual soldiers punishable. See for a discussion of different philosophical concepts of responsibility (Williams 2009; Risser 2009).

The criteria for evaluating good conduct in the Jus ad Bellum and Jus in Bello contexts are different. In the case of military technology development and weapons design, a wider variety of different types of actors share in a common moral responsibility. As noted in the introduction, trends in converging technologies and open innovation could give rise to a need to broaden the scope of relevant research and technology development beyond explicitly military technology development and weapons design, in order not to overlook developments with foreseeable future evil effects. However, the relevant types of actors that should share in the responsibility are different in each of the distinct domains of military technology development, civil research not aimed at security and civil security research.

Military Technology Development

Traditional ethical JWT reserves the authority to deciding on matters of war and peace for the sovereign states that are responsible for protecting state security and the human rights of their citizens. New military technologies—technologies from the prototype stage developed specifically for use by the military forces—are intended to be used in a context of international armed conflict, with foreseeable evil effects. However, sovereign states may need to develop these technologies in order to continue to defend the integrity of the realm; this includes protecting the human rights of their citizens. An extrapolation of the JWT would therefore exclusively reserve the right to decide on the development of these technologies for the legitimate governments of sovereign states and these governments' institutions. Given current trends in globalisation and construction of a system of international law, it is conceivable that such legitimate authority is no longer exclusively attributed to national governments. It could be extended by law to some specific supranational public bodies.[5] Responsibility could not be handed over to private industries and research bodies that are not controlled by the state: the bearer of legitimate authority.

[5] In current international law, apart from self-defence, a mandate from the Security Council is required for military action to be legitimate. In the future, European integration could lead to the transfer of authority the national to the EU level. A more thorough discussion on an adequate interpretation of the ethical concept of "legitimate authority" goes beyond the scope of this article.

Civil Research Not Aimed at Security

The JWT does not give any grounds for government intervention in civil research, as long as it does not have foreseeable implications for the security of the state or its citizens. The scientific community and industry are predominantly responsible for setting priorities in research that is not primarily developed for security applications. From an ethical perspective, the value of academic freedom dominates basic science. As the research becomes more applied in the development of innovative products and processes, it should increasingly be subject to economic values such as fair competition, the rights of innovating industries to protect their property and the freedom of choice for consumers. There could be legitimate reasons for government interference such as respect for human rights, the environment and the common good, as well as more mundane reasons like making available funding for research (as a collective good) from the public budget, addressing market failures, regulating market access, and increasingly promoting public dialogue.[6]

Civil Security Research

A person's right to life and security is a fundamental human right that can be threatened not only through the use of force by states, but also by individual citizens or private institutions or groups. Because it is a fundamental human right, individual citizens have the right to protect their own security if the state is not in a position to do so, including through the use of civil security technologies.

As in the case of military security, threats to civil security continue to evolve, calling for the development of new protective means, including but not limited to new civil security technologies. Because of their primary responsibility to protect their citizens' security, state governments take a leading role in priority setting for civil security research, but in a different capacity than in the case of military technology development. Because governments are not the only actors entitled to protect civil security, they are not the only ones who should share in a collective responsibility for civil security research. Moral responsibility for civil security research should be taken by a triple helix of the actors involved in this research including different governmental actors, industry and the scientific community.

To sum up, taking the JWT as starting point, different actors should be given responsibility for each of the three kinds of research. Governments of sovereign states are responsible for decisions on military technology development, given their exclusive legitimate authority for the defence of national security with armed force. Decisions on civil security research should be made by a broader group of actors where state governments have a leading but not exclusive responsibility, given their primary responsibility for justice and internal security inside their territory. Other actors can legitimately share in this responsibility on the grounds of fundamental

[6] Exactly what should be the responsibility of the state and what should be left to private parties is a political question that is answered differently in different countries and at different times. There is also a debate on democratising science: giving groups in society other than the scientific community and industry a say in research policy decisions. This debate goes beyond the scope of this article.

human rights. The responsibility to decide on other civil research cannot be claimed by or attributed to state governments merely on the grounds of the JWT.

Characterising Ethical Decisions

Having identified responsible actors for each kind of research, the next question this article examines is: What criteria included in JWT or other criteria are relevant to ensure that their decisions contribute to global peace and justice?

Military Technology Development

As argued above, military technology development has direct intended implications for matters of war and peace between states and should therefore be under the control of the institution responsible for deciding on this. In the traditional Jus ad Bellum chapter of the JWT, this is precisely the purpose of the criterion of legitimate authority. It is therefore proposed as a (deontological) criterion for the new part of the JWT for evaluating military technology development. However, not all possible decisions made by governments of sovereign states are beneficial to the human rights of their citizens. The JWT includes the criterion of just intent for evaluating the intrinsic ethical quality of decisions concerning war and peace. According to Moseley, "Just Intent" in the classical sense means that the reason for going to war should be to achieve justice including protecting its own existence, not to further self-interest or aggrandizement (Moseley 2009).

This deontological criterion is also relevant to promoting a review of the admissibility of decisions regarding military technology development.[7] Any investment in development of new military technologies is inherently future-oriented. Therefore criteria promoting a review of the consequences are also important elements of the JWT in the context of military technology development. A central consequentialist criterion is proportionality, common to Jus ad Bellum and Jus in Bello.[8] Its interpretation is adapted to the responsible actors and contexts. Military technologies are typically developed in peacetime circumstances under the authority of governments who have other responsibilities to their citizens and the international community besides national security. Proportionality should therefore ideally be understood to balance a variety of public goods such as future national security, the socio-economic interests of the country as a whole and the ultimate aim of global peace and justice.

[7] This criterion Just Intent should not be interpreted in a psychological way, but as the explicit or implicit purpose of the military technology in question (e.g. the apparent intent of a precision weapon is to limit collateral damage as much as possible, whereas the apparent intent of WMD is to indiscriminately create as many victims as possible).

[8] A commonly accepted requirement of new weapons developed today is that their effects should be scalable.

Civil Research Not Aimed At Security

As neither basic science nor applied research aimed at industrial applications is intended for security applications, the current deontological criteria of the JWT are irrelevant. However, several technologies that are primarily developed for peaceful purposes may allow for unintended dual uses that form a large-scale, disruptive threat to human and state security, in particular those technologies that can be misused for weapons of mass destruction. This threat is not inherent in the technology, but in the intentions of some of the people and organisations that have access to the technologies. Many scientists and industrialists are unaware of any military applications, whereas others aim for civil applications but are aware of potential or actual military applications. Finally, some scientists and industrialists contribute to the development of secondary military applications of civil research on purpose.

As an elaboration of the theory of double effect, the JWT promotes reviews of such indirect implications of civil research with potentially evil effects through consequentialist criteria. The JWT's consequentialist criteria—reasonable prospect of success, proportionality and last resort—are not suitable for evaluating dual use civil research.[9] This does not mean that an ethical evaluation of this research is not possible. As freedom is a core value driving both basic and applied research, a proper criterion for promoting reviews of dual use aspects of civil research could be balancing freedom and security. For example, Article 6 of the European Charter on Human Rights (EU 2000) states: "Everyone has the right to liberty and security of person." Discussion on the interpretation of this balance is already quite common among policymakers responsible for the governance of emerging technologies and ethicists alike.[10] Core values at risk and technology assessment could also be useful, such as responsibility, precaution and awareness adapted to dual use threats caused by intentions of individual or collective human actors.

Civil Security Research

Under International Humanitarian Law, the law of weapons is increasingly extended to uses of weapons by states in internal conflicts. From that legal perspective, there is no more categorical distinction between military and civil security technology development. This implies that if the ethical JWT framework is applicable to military technology development, it should also be applicable to civil security technology development.

However, civil security research is not undertaken in preparation for the use of force in international conflicts between states. This research is therefore not directly related to matters of war and peace. Given the absence of such a connection, the ethical JWT gives no compelling reason why the state—the bearer of the legitimate authority to decide on such matters—should reserve an exclusive right to take

[9] C.f. literature on codes of conduct for research, dual use life sciences and nanotechnology.

[10] E.g. in several EU funded projects including HIDE www.hideproject.org, RISE www.riseproject.eu and ETICA http://www.etica-project.eu/.

decisions on civil security research. The criterion of legitimate authority is therefore not relevant to this kind of research.

At first sight, two of the JWT criteria that are applicable to military technology development also seem relevant for promoting reflection on civil security technologies: the deontological criterion just intent and the consequentialist criterion of proportionality.

Furthermore, many technologies primarily developed for civil security also have a dual use aspect because the resulting products can be applied for civil as well as security purposes (e.g. biosensors for detecting both natural and human-made pathogens). Therefore the consequentialist ethical criteria proposed for evaluating civil research should also be used for civil security research.

The abovementioned analysis results in the proposition of a different set of criteria for different types of research: military technology development, civil research not aimed at security and civil security research. These sets of criteria are summarised in Table 1.

Examining Relevant Contexts in Actual Practice

After having discussed what aspects of the theory of double effect and the JWT could make it useful for an ethical assessment of nanotechnology development with military and civil security implications, the focus shifts to the relevant contexts in which the technology is being developed in actual practice. This section discusses the actors who are involved in practice and the technological developments of nanotechnology with applications in security and with applications in other sectors that have a dual use potential. Are the nanotechnologies that are targeted at security applications and those that are targeted at other sectors as distinct as the above philosophical categorization suggests?

Who are the Actors in Practice?

It is one thing to designate actors with the legitimate authority to decide on particular types of research and technology development from a theoretical-ethical

Table 1 Criteria for an ethical assessment of security related technology development

	Military technology (TRL 6–9): the JWT criteria	Civil security research (TRL 6–9): mix of the JWT and other criteria	Civil research (TRL 1–9): other criteria
Deontological criteria	Just intent Legitimate authority	Just intent	–
Consequentialist criteria	Proportionality	Proportionality Balance freedom-security Dual use risk/technology assessment	Balance freedom-security Dual use risk/technology assessment

perspective. However, in practice the actors that take responsibility for such decision-making are not necessarily the same, as illustrated by the following discussions. This involvement of other actors complicates the application of the JWT to security related technology development, because the actor bearing the theoretical authority may not have the practical power to impose his decisions.

Military Technology Development

In the case of military technology development, decisions are commonly shared in the "military-industrial complex". This concept was first coined by U.S. President Eisenhower (1961), who reflected on the achievements of his Presidency. He warned against the "recurring temptation to feel that some spectacular and costly action could become the miraculous solution to all current difficulties. A huge increase in newer elements of our defence … these and many other possibilities, each possibly promising in itself, may be suggested as the only way to the road we wish to travel." "But each proposal must be weighed in the light of a broader consideration: the need to maintain balance in and among national programs…" Since WWII, the USA had newly created a permanent armaments industry and in conjunction with it, a sizeable defence sector. "In the councils of government, we must guard against the acquisition of unwarranted influence … by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist. …" (Eisenhower 1961).

The existence in many countries of such a military-industrial complex could hamper the ethical evaluation of weapons research that is obligatory for States Parties to the First Protocol of the Geneva Convention. The existence of this treaty does not guarantee that all weapons research is assessed, because private industry and States Non-Parties are not bound by these conventions. There are more guarantees that relevant research is assessed for biological and chemical weapons: States Parties to the Biological and Toxin Weapons Convention (BTWC) and Chemical Weapons Convention (CWC) must make production and development a criminal offence through national law that is binding for industry.[11]

Civil Research not Aimed at Security

On the other hand, a triple helix of science, industry and government is commonly held responsible for developing civil technologies. The relevant governmental actors are primarily departments of education, sciences and economic affairs at several governmental levels (national, local, regional and supranational). Nanotechnology is one of the first areas of research where in several western countries other government departments, including those responsible for protecting public health and safety and the environment, have become involved in the discussion on responsible governance at such an early stage of research and before the market introduction of the bulk of applications.

[11] C.f. BTWC: http://www.unog.ch/80256EDD006B8954/(httpAssets)/C4048678A93B6934C1257188004848D0/$file/BWC-text-English.pdf and CWC: http://www.opcw.org/chemical-weapons-convention/.

Civil Security Research

In Europe, at least, the traditional distinction between technology development for military and homeland security and for non-security related innovation is increasingly fluid. James analyses European policies on defence, civil security research and innovation and foresees a development towards open innovation combining civil and defence research as one of the possible outcomes by 2030. James (2010) observes that such integration is hindered to some extent by conflicting predominant values: academic freedom in universities versus national security in defence circles.[12] The development of a new area of civil security research may attract a new research community willing to bridge the divide between both communities (James 2010).

In all three cases the actors that should theoretically bear responsibility for decisions on technology development have to face influences and competition from other actors with the power to intervene. This is primarily a political process driven by changes in national societies and globalisation. But it is not the only force at work blurring the boundaries between the three distinct application domains of technology. As argued below, in our current age of convergence, technological developments are intrinsically boundless.

Trends in Nanotechnology with Security Implications[13]

Nanotechnology is an enabling technology that can be applied in a wide variety of sectors. The common denominator is the size of functional structures between about 1 and about 100 nm in at least one dimension. All sorts of materials can be structured or processed at nanometre scale. The development of nanotechnology requires the cooperation of physicists, chemists, materials scientists, biologists and other disciplines in interdisciplinary research projects and programmes.

Nanotechnology for Civil and Military Security

A wide range of developments in nanosciences and nanotechnologies have potential for military applications, including in nanoelectronics, nanomaterials and nanobiotechnology. These trends have been reviewed by several authors (e.g. Altmann 2006, Simonis and Schilthuizen 2006). Even though some of these nanotechnologies are developed specifically for military purposes, whether the research in question is formally classified as military, civil security or other research depends on the country's funding tradition. For example, some research that is labelled military nanotechnology in the US National Nanotechnology Initiative is similar to civil research in Europe. Explicitly military applications are only distinguishable as of the prototype stage (TRL 6–7 and higher).

[12] This presumed aversion of defence contracts in universities is contested by others.

[13] This section largely discusses trends in nanotechnology for civil and dual use applications that have been discussed in public literature, internet sources and events. Explicitly military nanotechnology was outside of the mandate of the project in which these information sources were reviewed. See for reviews of trends in military nanotechnology (Altmann 2006; Simonis and Schilthuizen 2006).

Ethically sensitive trends in nanotechnology that primarily target civil security include applications in border control, sensing, person identification, the protection of infrastructure and equipment, the detection of CBRNE (chemical, biological, nuclear, radiological and explosive substances) and the neutralization of their effects and decontamination (ObservatoryNano 2009). In border control, different types of biometrics instruments are applied. Biometrics can be defined as the "automated measurement of physical or behavioural characteristics to identify a person" (Ericson 2007). Examples are iris scans and finger prints. Nanotechnology is expected to enable next-generation biometrics, which will be miniaturised, integrated, multifunctional and efficient. In Europe, the European Defence Agency (EDA)'s Joint Investment Programme on Innovative Concepts and Emerging Technologies (JIP-ICET) is funding two defence-related nanotechnology projects: Novel NANOstructured optical Components for CBRN detection and high performAnce oPto-microwave links (NANOCAP) and a Personal biological Aerosol Tester for exposure Control with High efficiency (PATCH) (EDA 2009). Both are intended for products that can be used by the military and police forces, so it appears arbitrary to classify them as military technologies, except for the fact that military products are 1,000× as expensive as civil products. Another Joint Investment Programme, JIP-CBRNE, of the EDA will run parallel to a call for proposals on CBRNE in the thematic programme on Security in FP7, expected to be launched in 2012. A specific new trend in nanotechnology for security which could give rise to new ethical and societal issues is quantum cryptography. Quantum cryptography makes use of quantum physics to encode confidential messages. It can be used by the military and diplomats, where confidential communication and lasting uncertainty of whether confidentiality has been compromised is important. Another new relevant nanotrend is encoding materials (on-wire lithography, Roco et al. 2010). Nanotechnology instruments enable the physical writing of messages on tiny wires that have nano or micrometer sizes.

Dual Use Nanotechnology

Several applications of nanotechnology that have been developed primarily for the security sector can also be used outside this sector by industry or public services such as the fire brigade. For those applications, the technology used to protect security against attacks by human actors is hardly distinguishable from that used for protection of safety against natural or technological threats. These applications are a form of dual use of nanotechnologies. But the category "dual use nanotechnology" also includes technologies that are not primarily developed for security related sectors and have an intended or unintended secondary use that has implications for security. The relevant sectors include information and communication technologies, healthcare, aerospace and transport. Two main trends can be distinguished in dual use nanotechnology. The first is a general trend that civil and military research in emerging technologies overlap. In particular, the miniaturisation of Information and Communication Technologies (ICT) can be applied in both military and civil applications.[14] New trends in nanotechnology with a particular dual use character

[14] ICT R&D in Europe is located completely in the civilian sector because military demands are not more stringent than civilian.

include metamaterials and quantum computing. Metamaterials are materials with negative refractive index. This means that the light is wrapped around the object made of this material turning it invisible. The same property can also be applied in lenses focusing light. Potential applications are in satellite antennas, biomedicine, biosensing and ultrasound imaging.[15] Quantum computing is a form of parallel computing based on quantum mechanics. Quantum computing is expected to have an exponentially larger computing power than conventional computing. Metamaterials and quantum computing are still in the basic research phase. Recent technological trends including nanobiosensors and nanowires are also dual use: they can be applied in both medical diagnostics and bioterrorism monitoring.

The second trend in dual use nanotechnology is the potential implications it may have for current international treaties forbidding biological and chemical weapons of mass destruction and the proliferation of nuclear weapons. These implications can be positive, in CBRN sensors, vaccines and medication that make it easier to detect the presence of these Weapons of Mass Destruction (WMD) or protect against their impacts. The same sensor technologies and pharmaceutical platform technologies needed for protection against CBRN weapons are needed in medical devices and pharmaceuticals for natural diseases. On the other hand, experts have warned against civil technological developments that may undermine the treaties including microreactors for manufacturing chemicals, bionanotechnology and synthetic biology (Üzümcü 2010, Altmann 2006 and Nixdorff 2010).

The examples of nanotechnologies given above illustrate that there are no clear technological boundaries between technologies for military, civil security or other applications. The next two sections give an analysis of the key controversies that can be found in current debates related to nanotechnology for security applications and dual use nanotechnology. These issues are subsequently assessed against the proposed JWT criteria for different categories of research and technology development.

Current Debates Related to Nanotechnology for Security

In Europe especially there is an ongoing debate among policymakers and stakeholders on the political and societal aspects of current security policies The European Union has only been allowed to invest specifically in civil security technologies under the Framework Programme for Research and Technology Development (RTD) since about the last 5 years; therefore there is considerable interest in the ethical and societal issues raised by these security technologies. In these debates, nanotechnology is not considered to raise particular distinct concerns.

Political Issues

Governments and the European Union have an obligation to protect the human rights of their citizens. These rights include the rights to liberty and to security. However, determining what would be the proper balance between those rights is a

[15] www.nanowerk.com.

political question to which the answer has varied through history. Since the attacks on the World Trade Centre on 11 September 2001, the protection of citizens and state security against organised crime and terrorism has been given more weight than individual liberties. This political choice is backed by considerable public support. For example, more than half of respondents in the 25 EU member states in 2007 considered the fight against organised crime and trafficking and the fight against terrorism to be major concerns. Less than a quarter were very concerned about promoting and protecting fundamental rights, and about the quality of justice (European Commission 2007). By 2010, 75% of the respondents in the EU-27 backed the Common Defence and Security Policy and terrorism ranked fourth in the list of main concerns for the European Union; 15% of the respondents considered this to be among the two main concerns (European Commission 2010).

However, the fact that European citizens support the EU security policy in general does not mean that they also support the development of security technologies. A number of Non Governmental Organisations (NGOs) are currently raising concerns about the privacy and human rights aspects of the information society. Recent stakeholder debates on ubiquitous computing or ambient intelligence have been sparked by the use of Radio Frequency IDentification (RFID) chips as tags in increasing numbers of products, including consumer goods, as well as passports, public transport cards and implants in the human body. In a Dutch public debate on the vaccination campaign for the H1N1 influenza in 2009, some expressed the fear that the government might use this campaign to implant nanochips into the bodies of citizens.[16] The same issue has been raised in France by the CNIL (National Commission on Informatics and Liberties) and in other countries and the internet discussion forums. NGOs' concerns focus on body scanners and biometrics in border control, surveillance, "big brother" legislation and the international exchange of data for fighting crime and terrorism. No NGO participating in any public dialogue has taken a position explicitly mentioning nanotechnology based security technologies.[17]

Ethicists engaged in discussions on security technologies tend to focus on surveillance issues. The discussions of biometrics in the Homeland Security, Biometrical Identification and Personal Detection Ethics (HIDE) project and in the Nanoforum report on nanosecurity (Nanoforum 2007) have identified Ethical, Legal and Social Aspects (ELSA) intensified by nanotechnology. In particular, terahertz detectors give rise to severe privacy and human rights issues if used to see through clothing. It is not very clear what the main market is for security technologies. Governments may be dominating the research, but small shop owners wanting to prevent theft might well represent a larger market for some affordable end products.

[16] Dutch newspapers reported on this discussion, e.g. *Trouw*: http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1177074/2009/12/28/rsquo-RIVM-stond-er-te-vaak-alleen-voor-rsquo.dhtml and *HP/De Tijd*, http://test.hpdetijd.nl/2009-11-09/zeven-vragen-over-de-mexicaanse-griep.

[17] E.g. EDRI website, Digital Civil Rights in Europe, http://edri.org/.

Research Ethics

The discussion on the priorities in security technologies funded under the EU Framework Programmes for RTD has included ethical aspects from the beginning. The European Security Research Advisory Board (ESRAB 2006) recommended research into 'ethical aspects of security technologies' and a 'review of existing codes of conduct, best practices, etc. as to the ethical use of security technologies and to develop new ones where shortfalls exist.' Research in social sciences and humanities must furthermore contribute to the development of new Privacy Enhancing Technologies, and to criteria for assessing if new technologies respect citizens' rights and current legislation. Such research must also enable early identification of a need for new or adapted legislation. These recommendations have been implemented in the form of a number of projects that investigate ethical and societal aspects funded under the 7th European Framework Programme for Research and Technology Development (FP7). Some of these projects have included nanotechnologies for security applications.

Five years after the ESRAB report, the incorporation of security research in the European Framework programme has given rise to new policy issues. Therefore, President Barroso of the European Commission has requested an opinion from the European Group on Ethics in Science and Technology (EGE) on the ethical implications of security technologies.[18] The European Commission is developing a code of conduct for security technologies.[19]

Current Controversies Related to Dual Use Nanotechnology

There is eternal tension between the civil and military applications of dual use technologies.[20] Currently there are two main controversies related to dual use technology that are not addressed adequately in public or stakeholder debates. Even though these controversies are general, they are especially relevant to dual use nanotechnology. The first controversy has to do with the proper relationship between military and civil security R&D. It has not been addressed because there is no neutral meeting ground where representatives of peace movement and defence circles can explain their concerns and discuss viable solutions. The second controversy focuses on the proper response to the potential misuse of nuclear, biological and chemical research and industrial facilities, knowledge and products for weapons of mass destruction (WMD) by terrorists or hostile states. For example, Blank discussed the "laboratories on a chip" currently used as an in vitro health test. In the future the whole system in a container could be injected into the body for in vivo detection and therapy. This technology is inherently dual use (cited in Malsch

[18] On 22 March 2011: http://ec.europa.eu/european_group_ethics/index_en.htm.

[19] René von Schomberg, intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, http://www.etica-project.eu/.

[20] "Dual use" is traditionally a term that implies that certain technologies or other resources can both be used for civil and military applications. However, in philosophical debates, "dual use" can also mean that a technology can be used for good and bad purposes, where the distinction between military and civil uses is not made (C.f. van der Bruggen 2011).

and Fruelund-Andersen 2011) Even though these issues are addressed in regular meetings between states parties to WMD treaties and in legal or voluntary measures imposed on the scientific community by national authorities, many relevant aspects are not addressed openly.

Relationship Between Military and Civil Security Technology

Discussions on the relationship between civil and military security R&D have entered the agendas of both the peace movement and defence circles. There is not much interaction between the peace movement and defence circles. The peace movement stresses the categorical distinction between military and civil technologies, whereas defence circles stress technological similarities and synergies.

In the peace movement, Vlandas (2006) tabled a discussion in the NGO Scientists for Global Responsibility (SGR) on the governance of nanotechnology in order to prevent negative environmental, security, health or social impacts. He was especially concerned about secret commercial and military research and hoped that whistleblowers could give timely warnings of negative developments. SGR has been working on a project warning against military influences on research since 2003. Another issue discussed in the peace movement is the opportunities offered by civil applications of R&D in nanotechnology for preventive arms control directed at dangerous military developments (e.g. Altmann 2006). More recently, the International Network of Engineers and Scientists for Global Responsibility (INES) started a campaign in January 2011 calling on researchers to reject research for the military by signing an appeal to the heads of universities and responsible academic bodies. This campaign builds on a debate in Germany on the "civil clause" in universities' constitutions that has been ongoing since the merger of the Forschungszentrum Karlsruhe (with a civil clause since its foundation in the mid-1950s) and the University of Karlsruhe (without a clause) to apply the clause right across the new Karlsruhe Institute of Technology (INES 2011).

On the other hand in European defence circles, the European Defence Agency (EDA) has been promoting better integration under the European Framework Cooperation between European Defence Research & Technology (R&T) programmes and Civil Security R&D programmes, including FP7 and ESA (EDA 2009). Similarly, the European Commission's policy for strengthening the European security industry also includes promoting synergies between civil and defence technologies (European Commission 2010). The European Parliament "strongly supports the establishment of synergies between civil and military capabilities" … "the EDA [European Defence Agency] should play an operational role in developing dual technologies and civil and military capabilities … inter alia, the security strand of the Framework Programme for Research and Technological Development could serve as a basis for developing such synergies" (Article 69 of the EP).

Neither side appears to defend its positions through ethical argumentation. Framing the issues from a JWT perspective, as discussed in the present article, offers arguments for evaluating both positions and improving decision making. This assessment will be made in Sect. "Contributions of the JWT to the discussion" below. The analysis of controversies will continue with the other issue, WMD, first.

Weapons and Materials of Mass Destruction

The discussion on the responsible governance of weapons and materials of mass destruction includes international legal and political aspects, as well as issues related to emerging technologies. There is interest in the potential positive and negative impact of developments in nanotechnology for the Chemical and Biological Weapons Conventions (CWC and BTWC). For example, in 2008, the Scientific Advisory Board (SAB) to the Organisation for Prohibition of Chemical Weapons (OPCW) reported on eleven relevant trends in science and technology, including in nanotechnology: "Advances in particle engineering and nanotechnology may lead to more effective delivery systems." The SAB concluded that a major offensive programme would be required to convert a new biologically active toxic chemical into a chemical weapon; therefore, this is not a pressing concern (OPCW 2008).

How to govern dual use technologies with WMD potential is another key issue in the discussion. The issues under discussion include an adequate definition of "dual use" in relation to biosecurity, preventing the technology transfer of dual use goods and technologies, the emergence of amateur science and the risk that science and technology may be used by terrorists in the future. Nanobiotechnology is often mentioned as one of the relevant emerging technologies, but is not a main concern at the moment.

Other Issues

A related issue raised mainly by civil security measures and technologies is the right balance between the fundamental right to security and freedom in specific cases, e.g. restrictions on academic freedom, trade restrictions and the infringement of surveillance on privacy. Roco and Bainbridge (2003) expected nanotechnology to contribute to (US) "national security in an age of asymmetric warfare and terrorism, through global surveillance and universal tactical and strategic awareness. This constitutes a revolution in military affairs, in which the whole idea is to take small groups of people and put enormous capability in their hands through very small systems. Yet this may also lead to a loss of privacy among those whose security is protected, through very large databases, quantum computation, decryption and universal genomics."

More futuristic concerns have to do with the use of remote control or autonomous combat robots and soldier enhancement, implants and brain-machine interactions. Homan foresaw that military robots would be increasingly enabled by miniaturization in the semiconductor industry. Military robots are used for dirty, dull, difficult and dangerous work and to address the increasing lethality of warfare and the proliferation of weapons of mass destruction. Blank expected intelligence for robots to need supercomputers enabled by nanotechnology; i.e. quantum computing (cited in Malsch and Fruelund-Andersen 2011).

Contributions of the JWT to the Discussion

There is a stark contrast between the perspectives inspired by the ethics-based JWT and by a technological analysis of security related nanotechnologies. The framework of the JWT suggests categorical distinctions between the development of military technology on the one hand and general civil research and technology development on the other. Such distinctions appear to call for making both types of developments subject to distinct governing regimes. In theory, civil security research has characteristics that require it to be treated as both military technology and characteristics that require it to be treated as civil research.

Nanotechnology, on the other hand, has from the outset been conceptualized as a container term that encompasses a wide range of materials and devices developed in interdisciplinary cooperation, involving a variety of scientific disciplines, with almost universal applicability. From this perspective, the boundaries between military, civil security and non-security related nanotechnology appear to be arbitrary. Those nanotechnologies that are expected to have military or civil security applications are discussed as promising for both and likewise for non-security related applications. The same infrastructure and expertise can be used for all three categories of applications.

The assessment in this section is made in the same order as above, from the specific development of nanotechnology for security applications to more general distinctions between civil and military research.

Nanotechnology for Security

As argued in Sect. "Trends in nanotechnology with security implications", broad public support for government policies that protect security does not imply acceptance of technological instruments used to further this goal. Civil society criticism of particular devices and technologies such as biometrics is based on ethical assessment of its implications, such as privacy, surveillance and proportionality. Such discussion tends to start relatively late, when technologies are already in use. Experiments with privacy enhanced technology design are attempts to integrate the discussion in earlier stages of technology development, as a means to reduce their controversial nature. Privacy enhanced design is already commonly accepted among engineers and philosophers alike.

A remaining problem is how to properly integrate a broad ethical reflection into the existing selection process of projects on the development of security technologies. The theory of double effect and its elaboration in the JWT criteria can shed light on dilemmas in research ethics for security research. From this perspective, any proposal for civil security research should be scrutinized with respect to the intention for which it is undertaken as far as this is apparent from the explicit or implicit purpose for which the technology is eventually to be used. Is the research intended to contribute to a more just and peaceful society that respects the human rights of all citizens? In the present organization of ethical reviews of FP7 projects, an assessment of the explicit and implicit intentions of projects is not foreseen. If the European Commission wants to improve this ethical review, it would be advisable to include the criterion of just intent to specifically evaluate the aims stated and intended effects of both the proposed research and the resulting security products.

The consequentialist criterion of proportionality necessitates an assessment that compares the projects proposed with other, technological and non-technological solutions to current and foreseeable civil security needs. Proportionality is already a requirement for assessing the acceptability of security technologies with privacy implications.[21] It could be included in the proposed EC code of conduct for security research, together with the criteria that civil security and dual use research have in common: balance freedom and security and dual use risk/technology assessment.

Dual Use Nanotechnology

What constitutes a proper relationship between military and civil research from the perspective of the theory of double effect and the JWT? The key criterion that distinguishes military from non-military technology development is that technologies applied explicitly to military purposes are under the control of a legitimate authority.[22] This requirement of control by a legitimate authority is equally valid to publicly and privately funded military research.

Integrating organisations or research programmes for military and non-military research that once were separated makes it cheaper and easier to use technologies developed primarily for non-military applications and secondly for military applications. Therefore the need for control by a legitimate authority is expanded to encompass those technologies, in addition to traditional military technologies. Imposing such control is likely to increase the economic or social cost of civil research. Interestingly, for civil security technologies and ICT, the need for more expensive privacy enhanced design is commonly accepted; also by policymakers and engineers. The need to respect contemporary ethical and legal requirements may give rise to increases in the economic cost of developing the technology but this is mostly not deemed problematic. Paradoxically, defence circles that call for the integration of civil and military research defend their position focusing narrowly on the economic benefits resulting from expected lower development costs of military technologies. Those peace activists contemplating research policies appear to value academic freedom above all else. Neither appears to reflect on the ethical and philosophical grounds supporting either position. The JWT requirement of state control over military technology, together with the common criterion of proportionality, suggests that an economic cost-benefit assessment should take into account the difference in costs for military and civil research in an integrated and separated system. For such a balanced consideration, general forums such as plenary parliamentary debates and open stakeholder dialogues are more appropriate than specialised parliamentary committees and interest groups.

[21] Discussion at RISE/HIDE workshop on the 9th and 10th of December 2010.

[22] In classical JWT, this would be the legitimate government of a sovereign state. Under International Humanitarian Law, legitimate authority may not be limited to national governments, but may also be attributed to some specific supranational bodies. A discussion on the right interpretation of the ethical concept “legitimate authority” goes beyond the scope of this article.

The JWT requirement of just intent is common to military and civil security research. It calls on both defence circles and peace movement to reflect on the aims of their proposed policy and on the appropriateness of the means to achieve those ends. Purely economic grounds are not enough to justify integrating military and non-military research. And academic freedom alone is not enough to justify separating them. Under the JWT, any acceptable military research has to be explicitly aimed at increasing security. A decision to integrate or separate military and non-military research should contribute to a proper balance, optimising both security and freedom. The advantage of separating military and non-military research is that it makes is easier to control classified military research when a more limited group of actors has access to it. Furthermore there is less need to restrict the freedom of non-military researchers to prevent compromising security if the two types of research are confined to separate organisations or research programmes.

However, separating military and non-military research is not sufficient to exclude all security risks of non-military research, because the use of unclassified research results in academic literature for military purposes cannot be excluded totally. As argued before, research in nanotechnology and other technologies for primarily civil applications could be misused for WMD or conventional weapons. As the costs of certain types of dual use research decrease, these technologies may become accessible to an increasing group of states and non-state actors. Even if military and non-military research (or security and non-security research) is formally separated, dual use research in civil organisations may present a security risk. The JWT does not present arguments for imposing restrictions on non-security related research by applying deontological criteria derived from the Jus ad Bellum framework. But from the broader perspective of the theory of double effect, civil research with foreseeable dual use potential such as nanobiotechnology and nanoelectronics for controlling the external environment should be assessed against consequentialist criteria to promote beneficial impacts while minimizing the risk of misuse. This can be achieved by reflecting on the proper balance between the human rights to freedom and security and by applying risk and technology assessment methods, taking into account the fact that the dual use security risk is caused by human intention rather than technological properties.

Conclusion

This article has tried to adapt a framework of the ethical JWT to the development of research and technology, with implications for peace and security, including military and civil security technology development and civil research with dual use potential. The JWT is a special case of the theory of double effect. As such it could be useful for evaluating military technology development from the prototype stage, because it is undertaken in direct preparation for the use of force in international conflicts. The JWT presents a framework for evaluating actions aiming at a good purpose with foreseeable evil effects. It requires compliance with both deontological and consequentialist ethical criteria. There is no categorical difference between preparation for the use of force by a state in international and national conflicts (e.g.

civil war, oppression of own population, crowd control). Therefore, if a framework based on the JWT—with deontological and consequentialist criteria—is applicable to military technology development, it should also be applicable to civil security technology development. However, security is a fundamental human right and states are not always in a position to defend it. There is insufficient reason for the state to be the only actor with the legal authority to invest in civil security research. Other civil research is not intended for the use of force. Therefore there is no reason to apply the JWT to it. However, the dual use potential of such civil research may lead to foreseeable evil effects. This potential for double effects calls for the need to consider the consequences of such research at an early stage of development. In the current debate on the ethics of science and technology and the ethical, legal and societal aspects of research (ELSA), several ethical criteria are already commonly used to evaluate such consequences. These could be applied in an adapted form to dual use research. This framework for the ethical assessment of security related technology development has been used as a starting point to shed new light on current debates on the governance of new emerging key enabling technologies such as nanotechnology, with potential implications for the use of force in future conflicts. It gives arguments in favour of a different evaluation of military, civil security and other technology development and research and suggests some criteria that could be useful in ethical assessments.

Acknowledgments The collection of empirical data on technological trends, foresight, policymakers and stakeholder discussions and ethical and social science literature was supported by the EU in the ObservatoryNano project no. 218528. Comments and suggestions on an earlier version of this article by Marcel Becker and Wim Pelt and an anonymous reviewer are gratefully acknowledged.

References

Altmann, J. (2005). *Nanotechnology and preventive arms control*. Osnabrück: Deutsche Stiftung Friedensforschung.

Altmann, J. (2006). *Military nanotechnology: Potential applications and preventive arms control. Contemporary security studies*. Oxon: Routledge.

Altmann, J. (2008). Präventive Rüstungskontrolle. *Die Friedens-Warte, 83*(2–3), 105–125.

Eisenhower, D. D. (1961). *Military—industrial complex speech*. Michigan State University. http://coursesa.matrix.msu.edu/~hst306/documents/indust.html. Accessed 22 Sept 2011.

Ericson, L. (2007). *Introduction: Nanotechnology and biometrics, presentation at biometric consortium conference*, 13 September 2007. http://www.biometrics.org/bc2007/presentations/Thu_Sep_13/Session_II/13_Ericson_NANO.pdf. Accessed 31 Jan 2012.

EDA (2009). Annual report 2009. Brussels: European Defence Agency. http://www.eda.europa.eu/genericitem.aspx?id=621. Accessed 19 July 2010

ESRAB (2006). Meeting the challenge. The European security research agenda. Brussels: European Commission. http://ec.europa.eu/enterprise/policies/security/publications/index_en.htm. Accessed 21 Feb 2012.

EU. (2000). Charter of the fundamental rights of the European Union. *Official Journal of the European Communities* 2000/C 364/01 18/12/2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Accessed 28 Dec 2011.

European Commission. (2006). *Eurobarometer 66*. European commission. http://ec.europa.eu/public_opinion/archives/eb/eb66/eb66_en.htm. Accessed 22 Sept 2011.

European Commission. (2007). *Special Eurobarometer 266*: *The role of the European Union in justice, freedom and security policy areas*. Brussels: European Commission DG Communication at the request of DG Justice, Freedom and Security. http://ec.europa.eu/public_opinion/archives/ebs/ebs_264_en.pdf. Accessed 22 Sept 2011.

European Commission. (2010). *Eurobarometer 74*. European commission. http://ec.europa.eu/public_opinion/archives/eb/eb74/eb74_publ_en.pdf. Accessed 22 Sept 2011.

Greenwood, C. (1998). The law of weaponry at the start of the new millennium. In M. N. Schmitt & L. C. Green (Eds.), *The law of armed conflict: Into the next millennium. International law studies* (Vol. 71, pp. 185–232). Newport, Rhode Island: Naval War College.

Gsponer, A. (2007). From lab to battlefield. *Disarmament Diplomacy*, *67*.

Gubrud, M. A. (1997). Nanotechnology and international security. In *Proceedings 5th foresight conference on molecular nanotechnology*.

James, A. D. (2010). *Scenario report SANDERA: The future impact of security and defence policies on the European research area*. SANDERA project. Manchester: Manchester Institute of Innovation Research. www.sandera.net. Accessed March 2011.

Lawand, K. (2006). Reviewing the legality of new weapons. *International review of the Red Cross, 2006*, 925–930.

Leydesdorff, L., & Etzkowitz, H. (1996). Emergence of a triple helix of university—industry—government relations. *Science and Public Policy, 23*(1996), 279–286.

Lietzau, W. K. (2004). Old laws, new wars: Jus ad Bellum in an age of terrorism. *Max Planck Yearbook of United Nations Law, 8*, 383–455.

Malsch, I. (2011). *Ethics and nanotechnology: Responsible development of nanotechnology at global level in the 21st century*. PhD-thesis. Nijmegen: Radboud University.

Malsch, I., & Fruelund-Andersen, A. M. (2011). *Ethical and societal aspects of nanotechnology enabled ICT and Security Technologies*. Observatory nano project. http://www.observatorynano.eu/project/document/3525/. Accessed 22 Sept 2011.

Mangan, J. (1949). An historical analysis of the principle of double effect. *Theological Studies, 10*, 41–61.

McIntyre, A. (2011). Doctrine of double effect. In N. Z. Edward (Ed.), *The Stanford encyclopedia of philosophy* (Fall 2011 Edition). http://plato.stanford.edu/archives/fall2011/entries/double-effect/. Accessed 31 Jan 2012.

Moseley, A. (2009). *Just war theory. The internet encyclopaedia of philosophy*. http://www.iep.utm.edu/j/justwar.htm. Accessed 9 Feb 2012.

Nanoforum (2007). Nanotechnology for civil security. Nanoforum. http://www.nanoforum.org/nf06~modul~showmore~folder~99999~scid~476~.html? action=longview_publication. Accessed 19 July 2010.

Nasu, H., & Faunce, T. (2009). Nanotechnology and the international law of weaponry: Towards international regulation of nanoweapons. *Journal of Law and Information Science, 20*, 21 (online).

Nixdorff, K. (2010). *Technological developments of relevance to the BWC*: *What are we talking about? BioWeapons Prevention Project RevCon Discussions*. http://www.bwpp.org/revcon-techinfluence.html. Accessed 22 Sept 2011.

Nussbaum, M. C. (2006). *Frontiers of justice: Disability, nationality, species membership (The Tanner Lectures on Human Values)*. Boston: Harvard University Press.

O'Donovan, O. (2003). *The just war revisited*. Cambridge: Current Issues in Theology.

ObservatoryNano. (2009). *General sector reports*: *Security. ObservatoryNano project*. http://www.observatorynano.eu/project/catalogue/2SE/ Accessed 27 Jan 2011.

Risser, D. T. (2009). Collective moral responsibility. The internet encyclopaedia of philosophy. Last updated 14 Dec 2009, Originally published: 6 July 2004. http://www.iep.utm.edu/collecti/. Last accessed 15 Oct 2010.

Roco, M. C., & Bainbridge, W. S. (2003). *Nanotechnology*: *Societal implications—maximizing benefit for humanity. Report of national nanotechnology initiative workshop*, 3-5 Dec 2003, Arlington, VA, USA: NSF, http://www.nano.gov/nni_societal_implications.pdf. Last accessed 29 Oct 2010.

Roco, M. C., Mirkin, C. A. & Hersham, M C. (Eds.). (2010). *Nanotechnology research directions for societal needs in 2020*: *Retrospective and outlook*. Dordrecht: Springer. www.wtec.org/nano2. Accessed 31 Jan 2012.

Schmitt, M. N. (2005). Precision attack and international humanitarian law. *International Review of the Red Cross, 87*(859), 445–466.

Schummer, J. (2001). Ethics of chemical synthesis. *HYLE: International Journal for Philosophy of Chemistry*, *7*(2), 103–124. http://www.hyle.org/journal/issues/7/schummer.htm. Accessed 31 Jan 2012.

Simonis, F., Schilthuizen, S. (2006) *Nanotechnology*: *Innovation opportunities for tomorrow's defence*. TNO Science and Industry. www.futuretechnologycenter.nl. Update 2009: http://www.isoconnectors.com/defensie/. Accessed 22 Sept 2011.

Üzümcü, A. (2010). *Future challenges of the OPCW*. Address by Ambassador Ahmet Üzümcü, Director General OPCW, Global Security Research Institute, Keio University, Tokyo, Japan. http://www.opcw.org/search/?search=future. Accessed 22 Sept 2011.

Van der Bruggen, K. (2011) Part A: Possibilities or Intentions: The concept of Dual Use reconsidered. In S. Miller, M. Selgelid & K. van der Bruggen, *Report on Biosecurity and Dual Use Research; A report for the Dutch Research Council*. Delft: 3TU Centre for Ethics. www.ethicsandtechnology.eu

van den Hoven, J., & Vermaas, P. (2007). Nano-technology and privacy: On continuous surveillance outside the panopticum. *Journal of Medicine and Philosophy, 32*(3), 283–297.

Vlandas, A. (2006) Managing nanotechnology. SGR Newsletter, *32*. http://www.sgr.org.uk/resources/managing-nanotechnology Accessed 1 Mar 2011.

Walzer, M. (1977). *Just and unjust wars: A moral argument with historical illustrations*. New York: Basic Books.

Williams, G. (2009). *Responsibility*. The internet encyclopaedia of philosophy, Last updated 9 March 2009. Originally published, 19 July 2006. http://www.iep.utm.edu/responsi/. Accessed 15 Oct 2010.

Wils, J.-P. (2007). Dubbel effect. In M. Becker, B. van Stokkom, P. van Tongeren, J.-P. Wils, & L. van de Ethiek (Eds.), Assen: Van Gorcum.