Sci Eng Ethics (2014) 20:617–638
DOI 10.1007/s11948-014-9555-7

EDITORIAL

Considering the Human Implications of New and Emerging Technologies in the Area of Human Security

Emilio Mordini

Published online: 11 June 2014
© Springer Science+Business Media Dordrecht 2014

Introduction

This special issue of *Science and Engineering Ethics* is devoted to the ethical, societal and political implications of new and emerging technologies in the area of Human Security. Its aim is to address the wider implications of an altered security landscape. Specifically, and in accordance with SEE's main area of interest, contributions to this special issue focus on those ethical considerations warranted by scientific and technological advances in the field of human security. This includes, but is not restricted to, issues of privacy and data protection, control, trust, surveillance, authority, and freedom. Papers consider some of the ethical and societal challenges related to new and emerging technologies in the context of the Human Security Doctrine (HSD), as it has been initially formulated by the United Nations Commission on Human Security (UNCHS 2003). The HSD argues for a paradigm shift from understanding security based on tangible assets (e.g., national borders, goods, properties, etc.) to one based on intangible human values. "The focus must broaden from the state to the security of people—to human security. Human security means protecting vital freedoms. […] Human security connects different types of freedoms—freedom from want, freedom from fear and freedom to take action on one's own behalf" (UNCHS 2003, p. 1). This special issue provides a multidisciplinary overview of some of the issues that have become central to security debates, focussing particularly at the intersection between technology and human values.

E. Mordini (✉)
Responsible Technology, Paris, France
e-mail: emilio.mordini@responsibletechnology.eu

What is Security?

According to the ISO Advisory Group on Security, security is "The provision of protection against threats to people, physical assets, infrastructure, information and information technology assets including electronic networks and facilities, and to the movement of people and goods and related facilities. Security provides safety and facilitates business commerce and trade through the safe movement of people, goods and services. At the same time, by protecting people, business and government, security enhances freedom and protects individual rights, including the right to privacy" (ISO/IEC/TMB SAG-Security Secretariat 2005).

Simply put, security is the absence of danger, from Latin *securus* "free from care". In this sense, securities incorporates a range of factors, from material assets to intangibles such as fear, mistrust, lack of confidence, feelings of despair, or, alternatively, hope, trust, confidence, resilience.

Security is opposed to the fear of threat, but quite importantly it is a notion relating to a subjective state of mind, and relates to one's interpretation of environmental factors. Insecurity, on the contrary, refers to a troubled mind-set. It is relevant to consider security at the very fundamental level of the individual human being, but also at various more collective levels, such as communities, societies, and other forms of clustering and their interdependencies.[1]

The meaning of the term "security" has deeply changed from the Classic and Medieval periods to the modern and contemporary world although the notion itself has always been central to human societies. In pre-modern thought, security was rarely about protecting goods and material assets. Likewise the idea of security seldom concerned specific threats; rather it was related to the overall, philosophical and religious, awareness that there are many things that lie beyond the influence of human actions.

The ancient Greek expressed this notion by using four different terms (1) *arkeo*, which means "protection"; (2) *eruma,* which is the military security; (3) *asphales*, which is a concept related to something which stands, which does not fall; (4) *apemosyne*, which literally means "without worry". Interestingly enough, the god devoted to security was the god who provoked earthquakes, Poseidon the Securer (ἀσφάλειος), who was worshipped in Sparta and in Delphi (*Paus. 3.11.9*; *Inscriptiones Graecae V 1.559*). His cult is also well-documented for Athens and Attica. The Athenians even offered sacrifice to Poseidon the Securer in preparation for the evacuation of Attica during the Persian invasion of 480 BC, so equating earthquakes to catastrophic military events. Poseidon's function of being both the god who generates, and protect against, earthquakes and catastrophic events enlightens one of the main philosophical feature related to the concept of security. Security is always a double edge sword, a *pharmakon*, which could both save and kill.

A similar polarity could be observed also in the Roman–Latin world, where the god who presided over security matters was Janus, one of the most ancient and

[1] Evidently, security considerations will bear different qualifiers, nuances and interpretations depending of the level at and viewpoint from which it is considered.

mysterious Roman gods.[2] His name is related to the Latin word for "door" (ianua) and his worship was related to all "passages" and transitions in the widest sense. Depicted as having two faces, as the two sides of a gate, Janus was the god of beginning, more precisely the god who stands at the opening. He presided over the transition from war to peace, and from peace to war. The doors of his temple were open in time of war, and closed when Rome was at peace. Some authors (Shilling 1960) have argued that Janus presided over the beginning of war (and in this case the notion of security should be strictly interlaced with the idea of military power), others (Capdeville 1973) think the opposite, that he chiefly presided over the return to peace (and in this case the notion of security should be connected to the idea of peace). With Janus one is then faced, in a still more radical way, with the inherent ambiguity of all notions related to the idea of security. In other words, war and peace, security and insecurity, turn out being anything but the two sides of a same coin.

The word security (in Hebrew: batach–*baw-takh'*) is very rarely used in the Bible, when it does occur it is present chiefly in the Psalms to represent God as a shield, as a secure harbor for humans, because human beings could trust only in God. In the biblical culture, the idea of security almost overlaps with the notion of trust and this is another important feature of the security/insecurity polarity which still survives. As society progressed towards secularization, the concept of trust became more and more immanent to the point that the modern state inherited most of the functions once provided by religion. Providing a secure harbor for its citizens became a standard prerogative of the modern State, which took over the role of religious authorities and received its legitimacy also from its role of "securer". In the early seventeenth century, Thomas Hobbes argued that the power of the State is justified by the theoretical concept of a social contract in which people freely agree to obey state authority in return for peace and security. The same line of thought was followed by subsequent modern political thinkers from John Locke through Jean-Jacques Rousseau to John Stuart Mill.

Also in New Testament the word security is very rarely used, probably the more important example is from 1 Thessalonians 5, 2–3, in which Paul warns his readers that "the day of the Lord so cometh as a thief in the night. For when they shall say, peace and security (*pax et securitas*); then sudden destruction cometh upon them". This enigmatic sentence has been connected to a famous, and still more puzzling, passage in 2 Thessalonians 2, 1–11 in which Paul describes the "end of times" and a mysterious power, the *katechon*, which would oppose the coming of the Antichrist, in such a way preventing also the final coming of Christ (which is expected to follow the Antichrist). In other words the *katechon*, literally what or who withholds, protects against the catastrophe, but in the same time it prevents the coming of a new era of peace. One is faced again with the dichotomy inherent to the concept of security, which is in the same while "secure and insecure". This poses a basic question on the legitimacy of State's claims to provide security to its citizens, in fact it is apparent that the border between providing security and defending the status

[2] Janus is not identifiable with any Greek god and was enigmatic even to ancient scholars (Capdeville 1973).

quo is often blurred. Starting with the German political philosopher Schmitt (1942, 2003) the notion of *katechon* has become an important concept also in political philosophy, notably in the analysis of the legitimacy of securitization policies (Virno 2008; Agamben 2013; Cacciari 2013).

The Golden Age of Security

"When I attempted to find a simple formula for the period in which I grew up, prior to the First World War I hope that I convey its fullness by calling it the Golden Age of Security". This is the well-known incipit of Stefan Zweig autobiography, *The World of Yesterday* (Zweig 1939–1942), one of the most celebrated books on the "Great Vienna" and its age. Zweig's quotation illustrates to what extent security became a collective worry at the beginning of the last century. "This feeling of security—continues Zweig—was the most eagerly sought–after possession of millions, the common ideal of life. Only the possession of this security made life seem worthwhile, and constantly widening circles desired their share of this costly treasure" (Zweig 1939–1942, p. 1).

By describing the twilight of the Habsburg Empire, Zweig also describes the complex web of relations between the notions of security, technical and scientific progress, and economic development. There are some points that deserve to be analysed in details because of their relevance to the contemporary debate on security.

First it is apparent that notion of security, as portrayed by Zweig, embraces many human activities which go well beyond the limits of national security. Zweig tells us that the central idea that shaped security worries in the Habsburg Empire was the idea that "only the man who could look into the future without worry could thoroughly enjoy the present". A similar idea will come back into the limelight of the security debate in the last decades.

Inherent to the idea of security as absence of worries about the future, there is the notion of risk. Risks should be distinguished by hazards. While hazards are a source of potential damage, risks concern the probability of harm. In other words, the notion of hazard focuses on external, unpredictable, events, while the notion of risk focuses on human activities aiming to avoid, mitigate and transfer damages. "The century of security—writes Zweig—became the golden age of insurance. One's house was insured against fire and theft, one's field against hail and storm, one's person against accident and sickness. Annuities were purchased for one's old age, and a policy was laid in a girl's cradle for her future dowry" (Zweig 1939–1942, p. 1).[3] According to Bernstein the shift from the concept of hazard to the concept of risk is the hallmark of modernity. "The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future

[3] Rigorously speaking the notion of risk is made up of the probability of occurrence of an event multiplied by the magnitude of the value or cost of the event. If one considers the number and severity of pogroms, which killed and raped thousands of Jews, that occurred in the Habsburg Empire, one could find difficult to totally agree with Zweig. However pogroms were chiefly events of the periphery of the Empire and actually an affluent Jews family, living in Vienna at beginning of 1900, could simply ignore them.

is more than a whim of the gods and that men and women are not passive before nature (…) The transformation in attitudes towards risk management unleashed by their achievements has channelled the human passion for games and wagering into economic growth, improved quality of life, and technological progress" (Bernstein 1996, p. 1).

Zweig mentions then another feature of the old Vienna, which he puts in relation with the "Golden Age of Security", the "pleasure in the theatrical, whether it was on the stage or in reality, both as theatre and as a mirror of life" (Buzan et al. 1998). The relation between the pleasure in the theatrical and the search for security is indeed deeper than one could suspect. The same idea of security is (at least in part) a discursive construct, which needs to be articulated through storylines, narratives, and images. There is no need to espouse the analytical framework of "securitisation" to see to what extent public feelings of security/insecurity are rooted in, and nurtured by, collective narratives (Schneir 2008; Baudrillard 1995). Narrative is basic human instrument to handle uncertainty and create meanings;[4] it is then obvious that it is used as a primary tool to deal also with security/insecurity.

Finally another crucial feature of the security narrative in the "Golden Age of Security" was the "the daily new wonders of science and technology". Any optimistic account on human scientific and technological progress is no longer tenable in the contemporary world, it is however difficult to escape from the impression that—although in different forms and by using different communicational codes—the notion of security is still deeply interlaced with science and technology wonders. The point will be however discussed in a specific, further, chapter of this introduction.

From National Security to Human Security

"To-day, now that the great storm has long since smashed it, we finally know that that world of security was naught but a castle of dreams" (Zweig 1939–1942, p. 1). The "Golden Age of Security" could not survive the Shoah, two world wars, a countless number of local and unusual (cold, asymmetric, on terrorism, on drugs, etc.) wars. To be sure, since then the Western obsession for security has become still more pervasive, but new security paradigms emerged, together with new perspectives about how security should be understood and enacted upon in the international community. If security relates to the notion of a sense of freedom from danger, and measures taken to assure safety or prevent harm, these objectives—traditionally considered within the remit of the state—are increasingly crossing boundaries.

[4] Narratives are not only explicit, intentionally created, "stories" (Fisher 1984). Humans understand themselves and their environment by representing them. Yet representation is never "objective", it is always permeated by desires, needs, fantasies, projects, generated both by the individual and the social group. Desires, needs, fantasies, projects, consciously and unconsciously, unavoidably restructure events into meaningful sequences, which are then coded into specific languages according to different cultural and professional contexts.

The change of focus followed decades of policy and research debates calling for a widening of the security agenda, in terms of perspective and in terms of the issues that may be considered as security threats (Buzan et al. 1998). A generalised feeling of "growing illegitimacy of traditional war-fighting", an emphasis on human rights, the emergence of new sources of insecurity, and the erosion of state autonomy with globalisation resulted in a long-term shift from 'war policy' to 'defence policy' to, finally, 'human security' policy (Glasius and Kaldor 2006).

The first mention of human security dates back to 1994, and focussed its critique on a post-cold-war argument about the deadlock of ideological conflict and the prevalence of national interests. The 1994 Human Development (UNDP) Report called for re-centring the notion of security around 'the legitimate concerns of ordinary people':

> The concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of nuclear holocaust. It has been related more to nation-states than to people. The superpowers were locked in an ideological struggle-fighting a cold war all over the world. […] Forgotten were the legitimate concerns of ordinary people who sought security in their daily lives. For many of them, security symbolized protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression and environmental hazards (UNDP 1994, p. 3)

In 2003 the United Nations established the *Commission of Human Security*, chaired by Sadako Ogata and Amartya Sen. At the completion of its work, the Commission presented its HSD:

> **The Commission on Human Security's definition of human security:** to protect the vital core of all human lives in ways that enhance human freedoms and human fulfilment. Human security means protecting fundamental freedoms—freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means using processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity. The vital core of life is a set of elementary rights and freedoms people enjoy. What people consider to be "vital"—what they consider to be "of the essence of life" and "crucially important"—varies across individuals and societies. That is why any concept of human security must be dynamic. And that is why we refrain from proposing an itemized list of what makes up human security (UNCHS 2003, p. 4)

This definition was arguably vague (Paris 2001, 2004), resulted both in antagonism from the more traditional supporters of (military) security, but also in growing interest from within the international relations and development communities which saw an opportunity to bring in new concerns under the high-urgency umbrella of security concerns.

In 2004, the Study Group on Europe's Security Capabilities proposed the *HSD for Europe*, which espoused the UN approach by stating that "a human security approach for the European Union means that it should contribute to the protection of every individual human being and not focus only on the defense of the Union's borders, as was the security approach of nation-states" (Study Group on Europe's Security Capabilities 2004).

At a first glance, the HSD in both UN and EU versions appears more ethically palatable than national security doctrines. But while the HSD reconciles security and human rights by making human rights the primary asset to be protected by security strategies, it also ends up turning the very notion of security into a fundamental human right. Consequently the pursuit of security is easily stretched so as to become congruent politics (Giddens 1990). This has its own risk. First, what kind of right is the right to security? On one hand, security could be conceptualised as a negative, liberty, right. In other words, the right to security could just entail the fact that state, or supranational, authorities, should restrain themselves from any action that might prevent their citizens from pursuing security in their daily lives. It is unclear, however, what pursuing security in daily life means. Either it simply means the exercise of all other fundamental rights, and in this case the notion of right to security would be pleonastic, or it means something more, but what? The most intuitive, and simplest, answer is that authorities should restrain themselves from using national security as an alibi for curbing fundamental rights: "States are now widely understood to be instruments at the service of their peoples, and not vice versa" (Annan 1999). Yet this answer has two tricky implications. First it implies a limitation of State sovereignty, which is not substituted by any true, legitimate, supranational authority (a vague and ill-defined international community cannot be considered a legitimate authority). Second, this may lead to the dilemma of the so-called "humanitarian intervention", whose legitimacy is often very arguable, notably when it implies the use of force.

Another possible answer to the question about the definition of the right to security, was provided by the 1994 UN document, which reads "Human security can be said to have two main aspects. It means, first, safety from such chronic threats as hunger, disease and repression. And second, it means protection from sudden and hurtful disruptions in the patterns of daily life-whether in homes, in jobs or in communities. Such threats can exist at all levels of national income and development" (UNDP 1994, p. 23). According to this answer, the right to security should be conceptualized as a positive, claim, right. In other words relevant authorities would have the duty to proactively protect their citizens against any major chronic threat and, in the same while, to prevent the risk of sudden and hurtful disruptions. The problem with this answer is that it widely enlarges the scope of security, which ends up by encompassing most human activities. Given the countless number of potential threats to human activities, a wide interpretation of the HSD would run the risk of plunging communities into an endless situation of humanitarian emergency, which may justify the mobilisation of means not necessarily accessible in a state of normalcy. In this context, the invocation of 'security' as a motive for intervention of corrective action can be seen as argument for ruling out some of the usual precautions taken in society. The overruling

strategic nature of security motives raises ethical concerns that have to be attended to. Moreover an ever-expanding area of security issues would run the risk to generate an obvious "crying wolf" effect: "Once anything that generates anxiety or threatens the quality of life in some respect becomes labeled a 'security problem', the field risks losing all focus" (Freedman 2004).

The idea of security as a positive right has however a sound foundation. The art.3 of the Universal Declaration of Human Rights (UDHR) reads that "Everyone has the right to life, liberty and security of person". Traditionally the reference to "security" has been read in conjunction with Article 25, "Everyone has the right (…) to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control", thus considering "security" chiefly as "social security". However, the inclusion of security in art.3 was also read in connection with World War II and totalitarianism (Morsink 1999) and notably in contrast with the notion of organic state and the overarching prevalence of "national security" on "personal security" in the Nazi regime. This justifies the further development towards a more comprehensive concept of right to security and human security. Yet, this also implies that the right to security could be legitimately understood as a positive right. This would be also consistent with the fact that "social security" is a positive right, consequently it seems logic that, extending the concept of right from social security to right to security at large, one will consider this right a positive right. Any positive right implies obligations, say, correlative necessary duties. Who has the duty to provide security to human individuals? According to the traditional doctrine, the duty to assist the right to security is bestowed by states and national authorities (see next chapter). This has increasingly moved the attention on state's duties: "Thinking of sovereignty as responsibility, in a way that is being increasingly recognized in state practice, has a threefold significance. First, it implies that the state authorities are responsible for the functions of protecting the safety and lives of citizens and promotion of their welfare. Secondly, it suggests that the national political authorities are responsible to the citizens internally and to the international community through the UN. And thirdly, it means that the agents of state are responsible for their actions; that is to say, they are accountable for their acts of commission and omission. The case for thinking of sovereignty in these terms is strengthened by the ever-increasing impact of international human rights norms, and the increasing impact in international discourse of the concept of human security" (International Commission on Intervention and State Sovereignty 2001, p. 7). Two further duty-bearer actors have emerged, the international community and the civil society. As vague as it is, the concept of "international community" has taken momentum in the last decades. Notably the notion of "international community" has provided legitimacy to intervention for human protection purposes and to the idea of universal jurisdiction, increasingly providing a framework for international action. Also the notion of civil society is ill-defined, it includes a vast array of non-institutional actors, such as NGOs, academia, citizens' organizations, human right advocates, the media, faith groups, etc. All these people have the duty, and the responsibility, to contribute to protect individuals (communities from terrorism and from mass killing, women from systematic rape, children from starvation, etc.), and

to participate in prevention of, and reconstruction after, crises (International Commission on Intervention and State Sovereignty 2001). This unavoidably leads to the issue of personal responsibility as far as personal security is concerned. If security is a personal positive right, there is also a correlative personal duty to protect it. In the next chapter I will discuss this point and the "security free-riding" dilemma.

Security and Liberty

The controversy between nation-centred and people-centred security leads to a huge ethical and political issue, which is the relationship between individual liberty and collective security. A standard narrative about security tells that one will pay security with liberty currency, say, the more one is secure, the less he is free. Although there is an undeniable tension between security and liberty, the reality is much more complex.

First of all one should distinguish between freedom and liberty. Freedom is a metaphysical concept that concerns free agency, say, whether human choices and actions are necessitated or free. If free agency is the capacity to will what is reasonable, a reasonable person is free even if he be a slave. This is not however the kind of freedom which is affected by the pursuit of security. Liberty[5] regards the relationship between individual and authority (political, legal, moral, religious, etc.). Liberty is freedom in relation to governing.[6] This idea emerged only in the modern age when individuals start to be seen as bestowed with rights apart from their social roles and independently from authorities over them.

Second, it is important to distinguish between external limitations and self-regulation, although this distinction can be tricky. Humans are full of limitations, which are inherent to their physical, mental and social structure. Some limitations are self-imposed in order to achieve some goals or to avoid some dangers. In principle self-imposed liberty limitations, with the goal to achieve more security, or to avoid specific hazards, should not be considered true liberty limitations, provided that one has not been forced by any external authority. Indeed self-regulation is often used by moralists as a paradigm of free agency. By self-imposing some limitations, humans would express at the highest degree their freedom from the instinctual or natural, realm. This is a nice statement but it is unfortunately false. If one analyses the granular structure of self-regulation processes, it is easy to see that they usually emerge from the internalization of societal, cultural, norms. In other words, very often, if not always, self-regulation is the most pervasive way of governing individuals because it runs below the level of awareness. Michel Foucault, who has developed the concept of "governmentality" to mean the whole

[5] "Liberty is freedom in the public sphere, freedom from captivity, oppression or despotic rule" (United Nations 2014).

[6] Etymology could help to understand. The verb "govern" (from Latin *gubernare*) originally meant to pilot a ship. A ship is directed by a coxswain. If one metaphorically equates life to a marine voyage and individuals to ships, who would play the role of the coxswain? The individual himself? His consciousness? External instances like religious or political authorities?

of practices through which individuals are governed, has devoted seminal pages to this issue. Interestingly enough, Foucault argues that freedom is necessary to the security apparatus (*dispositif*) because it "rather than imposing a binary of permitted and prohibited (…) establishes an average considered as optimal on the one hand, and, on the other, a bandwidth of the acceptable that must not be exceeded" (Foucault 2009, p. 21)

Finally, one should consider liberty limitations imposed by (external) authorities. The idea of authority comes from ancient Rome, where the term *auctoritas* covered various kinds of legal relationships. Who has *auctoritas* is the *auctor*, literally "the one who augments". The *auctor* augments (supports and complements) another's will and the notion of *auctoritas* was used for those cases in which an external power is needed to support one's own will. The model was the Guardian–Ward relationship. By extending this model from private relationships to the public sphere, *auctoritas* came to mean the juridical power to enforce laws and legitimate acts. For instance laws approved by Roman citizens needed to be enacted by the *Senatus* in order to be enforced (*auctoritas patrum*). Interestingly enough, this model equates citizens to wards and authorities to guardians. Likewise guardians, authorities take care of the affairs and personal well-being of other persons, who cannot act independently. Limitation of liberty is therefore integral to the idea of authority. In turn the authority, likewise a guardian, has the duty to provide support and protection. In other words, authority should not be confused with coercive power or with persuasion and rational conviction. Coercive power is based on mere power relationships and does not imply any liberty of the subject. On the contrary persuasion and rational conviction do not require any act of force to be performed. Authority is somehow in between. Of course one could argue that the notion of authority is purely fictional, because at the end the *auctoritas* always relies on power relationships and this concept just masks coercive power. This argument, which dates back to the ancient Greek sophist *Thrasymachus*, returns every now and then in the history of political philosophy and it has been variously raised also in the current debate on security. If one accepts the distinction between authority and coercive power, there are still two main possible perspectives. The first, which dates back to Hobbes, contends that authority is chiefly for providing human beings with enough security to live and carry out their businesses, by preventing the "war of every man against every man". The second approach, which dates back to Locke, contends that authority is chiefly for protecting individual liberty, which would be threatened by the strongest who would overwhelm the weakest. However, in both versions security and liberty would be goods whose protection legitimates the existence of authorities. Is there any inherent contradiction between these two goods? In principle there is not, because in case the contradiction would concern liberty and authority, rather than liberty and security. Provided that public authorities fulfil conscientiously their duties, their actions will increase both security and liberty, as least long term. To be sure, temporary limitations of one or both of these goods could become necessary. As a guardian could take some actions which may provoke some momentary discomfort to the ward, authorities could need to reduce either liberty or security in order to protect both, or achieve both at a higher degree, at a later moment. Is this picture over-optimistic? Probably it is, because

security and liberty do not appear to be protected and promoted to the same degree by public authorities. Liberty limitations, with the alleged objective to increase security, are definitely more frequent than security limitations, and—more worrisome—they tend to become permanent. Moreover, liberty is indirectly threatened also by the development of complex and pervasive surveillance systems, which are integral to the security apparatus.

Some scholars (Posner and Vermeule 2007) have recently proposed the so called "trade-off model" to explain the security-liberty relationship. This model, which is based—according to their claim—on empirical evidence, assumes that it would be impossible to increase security without decreasing liberty, and vice versa. Security and liberty would be continuously mutually exchanged. Preventing this exchange would be simply impossible, one should instead look for a right balance, a just trade-off between these two goods. "In welfare economics, the Pareto frontier, or contract curve, identifies a range of points at which no win–win improvements are possible: any change in policies that makes A better off must make B worse off. A similar frontier can be defined for liberty and security. […] At the security-liberty frontier, any increase in security will require a decrease in liberty, and vice versa. The problem from the social point of view is one of optimization: to choose the point along the frontier that maximises the joint benefits of security and liberty" (Posner and Vermeule 2007, pp. 26–27). The "trade-off model" has been variously criticized. For instance some authors (Schneir 2008) have argued that there is empirical evidence that security and liberty can be both, simultaneously, increased. This is not denied by proponents of the trade-off model,[7] who rather contend that there is a point beyond which it is impossible to make any one individual more secure without making at least one individual less free. Other scholars (Solove 2011) have argued that it is impossible to draw the security-liberty frontier (because there is not a metric, because security and liberty are not comparable, because liberty is not negotiable, etc.) and consequently the whole model would be of limited utility.

A still more radical criticism comes from scholars who deny the existence of "security" as a public good. This is the perspective chosen by the *Copenhagen School of security studies* (Buzan et al. 1998). According to these authors, security would be the name given to a process of social construction used to relocate a problem from the political sphere (international politics, social policies, etc.) into an area called "security". This process—overall described as "securitization"—would have the goal to legitimise the adoption of extraordinary means to handle that problem. Eventually scholars who refer to the securitization theoretical framework owe to Carl Schmitt the concept of state of exception, and to von Clausewitz the concept of war as another way of doing politics.[8] The "securitization" theory gets some important aspects of current security trends (which will be extensively

[7] "Of course not every issue of security policy presents […] a tradeoff. At certain levels or in certain domains, security and liberty can be complements as well as substitutes. […] [I]n some circumstances, it is possible that there are policies, other than the ones that government adopts, that would increase both security and liberty" (Posner and Vermeule 2007, p. 26).

[8] They extend von Clausewitz's argument to the notion of security, which remains to them chiefly a military notion.

discussed in various papers of this special issue) yet it is more descriptive than explanatory. Politics is certainly pervasive and most societal definitions are political in essence and depend on power relationships between groups, individuals, communities, at different relevant levels. Yet for this very reason the explanatory power of the securitization theory is limited, and the theory risks to be either redundant or uninformative. Once we have clarified that security is not an "objective" public good, but it is a speech act through which different actors intersubjectively agree to classify an issue as a security issue, do we have more instruments to deal with it?

An interesting implication of the security-liberty debate is the application of the "free rider problem" (Hardyn 2013) to security issues. In a nutshell the point is whether the 'calculation' of benefit (more liberty) and risk (less security) is relative to either a societal or an individual perspective. For a given individual it may well be more beneficial to refuse certain security measures, providing that a great enough part of the population take them. This could be the most rational course of action for the individual, although this course of action would be hardly morally tenable. For instance, exploiting the phenomenon of "herd immunity",[9] and provided that the community is mostly made up by vaccinated people, an individual may decide not to be vaccinated in order to avoid running any risk of vaccine side effects.[10] A free rider exploits collective solidarity in order to maximize profit. The security field offers many examples of free riding (Colombier et al. 2011). This depends on the fact that in large groups of people the benefit which originates from a security measure will not depend directly on one individual's contribution. Consequently the individual has an incentive to wait for others to contribute (and eventually do not contribute), in particular when the contribution implies some personal costs, or risks, or discomfort. This is hardly tenable in smaller, closer, groups, when other factors come into play, such as personal interactions, social control, mutual monitoring, altruism and commitments to each other. The more a community is cohesive and includes a limited number of members, the less free riding is practicable. On the contrary broken and disaffected communities facilitate free riding. In order to contrast free riding, authorities could either enforce coercive measures or promote more cohesive communities, in which it would be easier to make an appeal to "collective responsibility". In the security field both strategies are pursued. This mix between large scale coercion, social monitoring, and promotion of cohesive groups, could become very oppressive and detrimental to individual freedom.

[9] Herd immunity refers to the lowered probability of contagion occurring because of the high level of immunity in the community. If a large proportion of the population is immune, there is a reduced chance of transmission of the infection (but it depends also on the mode of transmission) and consequently a non-vaccinated individual is protected from the infection thanks his vaccinated fellows.

[10] This course of action is rational only to the extent that a few individuals take it, on the contrary the herd effect fades away and an individual's risk of being infected overcomes vaccination related risks.

Why Should 'Security' Matter to Scholars of Ethics of Technology?

Contributions to this Special Issue consider the relevance of security considerations to research debates related to the societal and ethical implications of new and emerging technologies. Why should "security" matter to scholars of Ethics of Technology? There are many possible answers to this question. A challenging one is provided by the German philosopher Martin Heidegger.

In his course on Nietzsche and the Nihilism (Heidegger and Krell 1991), Heidegger faces inter alia Descartes' philosophy and its relations with Nietzsche's idea of the will to power. The key point enlightened by Heidegger is the criterion that Descartes uses for defining truth, which is "certainty". Heidegger argues that the shift from the notion of truth to the notion of certainty is a "decisive milestone on the road that leads (…) eventually to Nietzsche's explicit doctrine of the will to power" (Davis 2007, p. 167). "Nietzsche himself explained Descartes's principle on the basis of the will to truth, and will to truth as a kind of will to power. Consequently, Descartes's metaphysics is indeed metaphysics of will to power, albeit an unwitting one" (Heidegger and Krell 1991, p. 237).

According to Heidegger, the connection between the notion of certainty and the development of modern technology, was prepared by Luther and the Reformation (Heidegger 1942), which also injected into that programme a specific obsession for security. Reformation's central concern was the will to salvation, say, how a person can be certain of his own eternal salvation, and Heidegger argues that "the will to salvation reduced religion to a matter of the subject's concern with his own security" (Davis 2007, p. 167). By ensuring a sound, mathematical,[11] foundation to the notion of certainty,[12] Descartes also prepares the shift from the notion of hazard to the notions of risk and security (Descartes 1989).

In short, Heidegger suggests that the lure for mathematical certainty, the obsession for security and salvation—which permeate today's techno-science—are different dimensions of a same, multifaceted, prism, which is ultimately the western will to power and its unavoidable failure.[13] In such a sense, security issues are central to ethics of technology, because any technology would imply, or may generate, security concerns, for the deep philosophical reason that any technology is (also) a (misleading) answer to the human, constitutive, ontological, insecurity.

However, reasons for interest in research debates related to the societal and ethical implications of new and emerging security technologies, are not only purely theoretical, but they also originate from rapid developments in a number of

[11] Descartes' concept of certainty is rooted in the idea of *mathesis universalis*, say, "a science of pure, naked quantities without any concrete reality, hence independent of imagination" (Sebba 1979, p. 62). There is, however, a longstanding discussion among scholars whether the notion of *mathesis universalis* was completely present already in Descartes or it was actually finalised only by Leibnitz (Doyle 2009).

[12] "Certainty today is not procured so much by the conventional method of deduction as, rather like the Cartesian credo, by the logic of double negation: all that can be excluded is that anything should be excluded (Ewald 2002, p. 289)".

[13] A similar argument—although from a quite diverse perspective—has been also used by Negri (1970) to argue that Descartes' metaphysics should be interpreted as a "political ontology", which contributed to provide the theoretical framework for the evolution from the mediaeval society to the bourgeois civilization.

technological areas that, directly or indirectly, affect the nature of security threats and responses. Globalization is characterized by the development of technologies which dramatically transcend national control and regulation, and thus also national security schemes. Moreover the increasing convergence between technological fields is generating a new technological context, which is changing the very nature of security responses. Novel technologies and their applications are also changing the profile of the major security threats. Increasing technological complexity often implies new vulnerabilities. Complex systems are the ideal target for disaffected groups, terrorists, mafia cartels, and one is probably destined to become more and more acquainted with terms such as cyberattack, cyberwarfare, and bioterrorism.

Technologies do not come free of value implications. They have to be approached in the context of their interpretation and of existing socio-cultural institutions. Because of their ground-breaking nature, questioning the ethical acceptability and the societal desirability of emerging technological applications appears as a matter of priority in the security domain. We will briefly discuss now those areas which will be further examined by papers published in this issue.

Information Technologies, Security and Privacy

The shift from analogic to digital has created a totally new category of objects, allowing translating into digits almost everything. This has amplified our capacity for storage and data processing to an extent which was simply unthinkable until a few years ago. Today information and communication technology (ICT) allows us to handle a huge amount of data, and to generate new information by merging and fusing archives and data sets. For instance, by observing and fusing publicly available data, such as web search queries, blogs, micro-blogs, internet traffic, financial markets, traffic webcams, Wikipedia edits, and so forth; it is possible to anticipate events such as disease outbreaks, financial and political crises, economic instability, resource shortages, and responses to natural disasters. However, this ability, which greatly improves our capacity to cope with different kinds of crises, is not without risks. The risk of creating self-fulfilling prophecies, nuisance alarms, function creep, misinformation, privacy and data protection breaches, increases as ICT becomes more sophisticated. Yet ICT is also an extraordinary instrument for empowering people, for creating and reinforcing community links, for stimulating democratic participation in a security crisis.

One of the main ethical conundrums generated by ICT in real life is the so-called "privacy paradox". The standard account of this paradox reads that, although people are increasingly concerned with privacy and data protection, they do not care about exposing themselves in the Internet, notably in social media. Büschel et al. (2014) address the privacy paradox from a peculiar perspective, say, the protection of online health data as a security issue. They compare psychological, ethical, and legal perspectives by using the notion of medical confidentiality as a paradigm to test different approaches. The conclusion is still an open conclusion, which advocates a holistic, transdisciplinary, approach that could bridge the existing theoretical gap.

Also Cavelty (2014) deals with a paradox in her paper devoted to cyber (in) security. She argues that current cybersecurity concepts and policies are actually generating insecurity. Her argument relies both on the experience developed in recent years starting with the NSA affair, and on theoretical consideration. From a practical point of view the author notices that most measures which apparently aim to protect the cyberspace are actually measures which create new vulnerabilities (she mentions, for instance, malicious software and backdoors purpose-made for cyberattack prevention and discovery). From a more theoretical point of view Dunn Cavelty challenges the current opinion that the cyberspace could be equated to a physical space. She finds the spatial metaphor rather misleading and she disputes the idea that we need a new covenant on cyberborders (the so called "cyber-Westphalia"). To her, the cyber is an area of free communication and considering it as a territory, on which each nation state should have the power to exercise its jurisdiction, "will almost inevitably have an impact on civil liberties, especially on the right to privacy and the freedom of speech". Eventually Dunn Cavelty uses the cybersecurity example as a paradigm to challenge the idea that nation state's security truly matches with citizens' security. This lead to the next papers.

With the next two papers we enter indeed in a more theoretical area, which is still related to ICT but which moves from ICT to open itself to wider reflexions on the ethical and philosophical foundation of security technology.

Kreissl (2014) takes a coherent navigation between security technology and technological security. Kreissl discusses most of the theoretical topics that have been faced in this introduction. Notably he is intrigued by the definition of security and its relationship with a more general understanding of human nature. Kreissl acutely perceives the deep link between the overall techno-science apparatus and the human security dimension. In such a context he uses privacy as a heuristic paradigm to unravel social interactions. To Kreissl, conceiving privacy as mere, legalistic, right is misleading, even risky for the very right that one aims to protect. As a matter of fact—he argues—privacy is first of all a cultural practice. This leads Kreissl to formulate the notion of an individual as a techno-social hybrid, and to pose a question about what it means to be human—Homme, Bourgeois and Citoyen—"in the age of encompassing surveillance". With this question, which echoes remote Marxian memories, he ends his dense paper.

Where Kreissl ends, Stahl et al. (2013) start. These authors investigate the possibility to use critical theory as "a critical lens" to highlight issues that traditional ethical theories tend to overlook. Critical theory approximately encompasses all those approaches that have been grouped by Paul Ricoeur under the broad heading of "school of suspicion": Marx, Nietzsche, Freud, and their successors, from the Frankfurt School to Michael Foucault. Stahl and colleagues test their approach in the context of Electronic Medical Records in the UK. It is particularly interesting, and thought-provoking, to consider Stahl and colleagues analysis in comparison with Büschel and colleagues previous contribution on privacy and confidentiality of online medical data. While Büschel and colleagues focused on the need to integrate different perspectives, Stahl and colleagues are more interested in unravelling aspects that are not usually considered, such as power relationships, questions about legitimacy, ownership, and empowerment. Stahl and

colleagues are however far from any political fundamentalism or ideological fanaticism. Their point is rather demonstrating the fruitfulness of unconventional approaches, which could provide broader theoretical basis and new practical insights.

Crisis Management and Response

The section devoted to crisis management and response groups two papers, which address two very different examples of emergencies.

Alexander (2013) is interested in crisis provoked by natural disasters, notably by earthquakes. As we have previously seen ("What is Security" section), earthquakes are integral to the western account on security and in ancient Greece the god who presided over security was Poseidon, the same god who was also responsible for earthquakes. Alexander's analysis starts from the 2012 earthquake in Italy and focuses on the role played by social media. Apparently social media played a role not so far from the (religious) function once played by the chorus in the ancient Greek theatre, because they chiefly commented and provided a collective voice on the events. Alexander points out that trust, communication, and reflexive representation, are essential to crisis and disaster management. Yet modern technology produces—together with new meanings and concerns, which are chiefly related to rapidity and magnitude of spread of information—also risk of misinformation, and the "death of discretion". The notion of the "death of discretion" is particularly intriguing because it implies arguments about privacy more subtle and nuanced than those currently used. As a matter of fact, privacy is not only a legal rule to be enforced or a fundamental right to be protected. If we take this concept seriously, privacy is a notion which deeply concerns civic society, social harmony, and mutual respect (Bird 2013). Adopting such an approach to the social media world could be rather demanding but it promises to be also extremely rewarding. Eventually, the main message provided by the author is that the immense potentiality of social media is still to be explored and that civil protection services should equip themselves to fulfil this task in the near future.

Similarities between natural disasters and catastrophic military events are evoked by Rebera and Rafalowski (2014) in their paper, which is devoted to the ethics of on the spot decision-making for first responders in large scale chemical incidents. For many reasons, chemical incidents are one of the most dreadful events that might occur, not the least because they would impose tragic ethical decisions. From triage decisions to the adoption of coercive measures, the spectrum of ethical momentous decisions in large scale chemical disasters is huge. Yet chemical incidents are less remote than one could imagine, they may occur both because of malicious intentions or as a result of natural and unintentional disasters. They require rapid and immediate decisions and don't grant time enough to develop sophisticated ethical conversations. Rebera and Rafalowski advocate the use of a broadly consequentialist approach, which could facilitate decision making process. They also suggest mitigating this approach with some previous deontological considerations, which could be even incorporated into the standard operational procedures

(SOPs) for first responders. The authors' interest is eminently practical, neither Rebera or Rafalowski aim to produce a general theory about an ethics of response to chemical incidents, rather they want to enlighten the main dilemmas involved in decision-making under the extreme pressures of circumstances and time. Finally Rebera and Rafalowski advocate a continuous, two ways, collaboration among practitioners and ethical experts as the sole possible solutions to ethical dilemmas in on the spot decision-making.

Dual Use in Theory and Practice

Technologies are changing our way of dealing with security threats, and how they can be addressed, within and beyond the realm of the use of military force. New threats and areas of exposure resulting from advances in both military and civil technologies challenge traditional notions of security, traditional disciplinary boundaries, and even boundaries between the military and the civilian. The field of dual use technologies is increasingly expanding, and it includes today most security technologies.[14]

Ilchmann and Revill (2013) discuss the issue of dual use from the peculiar perspective of chemical and biological weapons (CBW). CBW is an interesting example of the practical difficulties that one meets when one faces the current security discourse. Apparently CBW should not pose any major ethical or legal problems. If there is a weaponry sector strictly regulated by international norms which started almost a century ago, this is the CBW sector. Yet two main drivers are now challenging the CBW regime: changing security and changing science. The traditional normative framework was based on clear distinctions between peace, war, terrorism, organised crime, humanitarian interventions, etc. These distinctions are today increasingly blurred and less and less tenable. Moreover the rapid progress both in availability and power of enabling technologies, and their diffusion both across the globe and among unconventional actors, outside the traditional military research settings, are making it practically impossible to distinguish between civilian usage of research and its potential military applications. Authors provide some blatant examples, which concern, for instance, harassing and incapacitating chemical agents for policing purposes, the extensive use of herbicides in armed conflicts, the bioterrorism threat for propaganda purposes. Ironically enough, research on "humanitarian alternatives" to lethal weaponry is producing a new grey area of dual use technologies which escape any international regulation and ethical self-regulation.

Also Rath et al. (2014) address the changing scenario of dual use technologies, yet their approach is substantially different from Ilchmann and Revill. While Ilchmann and Revill are worried by the paradoxical effect of "humanitarian alternatives" to lethal weaponry, Rath and colleagues pose a basic question about definitions. They argue that the "term dual use is used today to describe different

[14] The ethical significance of taxonomies should not be underestimated. They are hardly technological issues; rather they depend on legal systems, governmental strategies, market structures, standards and specifications, industrial cultures, etc.

and even opposing framing". The aim of their paper is then to carry out a systematic evaluation and clarification of dual use concepts. The Authors identify four different polarities within the current usage of the term "dual use": (1) civilian versus military purposes; (2) peaceful v/s non-peaceful purposes; (3) benevolent versus malevolent purposes; (4) risks of misuse versus biosecurity. From each of these definitions one may derive practical, regulatory, consequences (including import and export regimes, legal sanctions, censorship of scientific information, etc.). New and better definitions will directly affect novel technologies which today run the risk of escaping from any international regulatory framework. It is the case of material technology and nanotechnology, which are developing new devices with unforeseen capabilities and are playing an enabling role in all other technology areas. It is also the case of biotechnology and synthetic biology, which are changing our way of conceptualising the life dominion, and are dramatically impacting most economic activities, including public health, farming and agriculture. In such a context Rath and colleagues emphasise the significance of adopting a HSD approach to the security issue. To them the sole possibility of addressing effectively new dual use dilemmas relies in overcoming short-sighted notions of national security and involving civil society into governance processes.

Unmanned Surveillance and Military Applications

The last section of this special issue is devoted to a special class of technologies, unmanned technologies. The term "unmanned" usually refers to machines without a person ("man") on board, without direct, physical, human control. The most frequent usage of "unmanned" is in relation with remote controlled, remote guided or autonomous vehicles (unmanned).

Although the systematic[15] use of Unmanned Military Technologies—notably unmanned aerial vehicle (UAV), commonly known as a "drone"—dates back to the Vietnam war in the mid 1970s (Radsan and Murphy 2011), they came into the public eye only in late 1990s, when their massive usage in the Kosovo war raised serious ethical and political concerns. After 9/11 the CIA started a specific research program (Eagle Program) on UAV, and UAVs have been increasingly and extensively used in warfare (overt and covert) operations, both for collecting intelligence and for carrying out armed attacks, either aiming at assassinating high profile individuals or inflicting massive casualties on the enemy without risking the life of pilots (Radsan and Murphy 2011).

Serious reasons for ethical concern were initially raised during the early Gulf and Kosovo wars. In both cases unmanned aircraft were widely used in war missions, chiefly for directing other aircraft pilots to target precision-guided bombs, and for gathering intelligence on enemy's troop movements. This led the French philosopher, Baudrillard (1995), to argue that the Gulf War was not really a war but manslaughter disguised under the false appearance of war. His argument was

[15] The first example of usage of drones in a war theatre was however in 1973 when Israelis used them to spot the artillery positions of the Syrian Army.

that the war did not almost take place from the point of view of western combatants, but in the form of propaganda imagery and media misrepresentation. A similar argument was then raised also by the Canadian writer and academic Michael Ignatieff in relation with the Kosovo war (Ignatieff 2000). Actually the case of the Kosovo war was particularly blatant. Around 13,421 people were killed during the conflict, including 462 Serb soldiers and a number of civilians comprised of between 488 and 527 people by NATO airstrikes (Krieger 2001). Against these figures, there was not a single NATO combat casualty. Ignatieff takes the Kosovo war as a paradigm of new high-tech warfare fought through remote control. He calls them "virtual wars", combatants are computer programmers, the nation is mobilised as a TV audience, and instead of formal declarations commencing and ceasing hostilities, there are only a start AND end of the game.

Noorman (2013) addresses the issue of Unmanned Military Technologies from the perspective of the principle of responsibility. He correctly points out that at the core of most ethical and legal questions raised by Unmanned Military Technologies there is the issue of individual and collective responsibility. "Taking the human out of the loop, trough increasing automation, will limit the ability of those who deploy, use and interact with the technology to control the outcome of events or to reflect on the consequences of their decisions". The central question is whether Unmanned Military Technologies are designed to be abused or whether it is possible to ensure their responsible usage. Noorman argues that there is room enough to negotiate responsible practices. He advocates a sort of "responsibility by design" approach, which is based on a distribution of responsibilities on many different levels, within and outside military organizations. Eventually Noorman thinks that whether or not human actors are held responsible for autonomous technologies is not the inevitable outcome of a blind technological development. On the contrary he argues that groups and individuals (including civilians and military officials, engineers and researchers) should negotiate established ways of holding people responsible of both the technical design and the application of unmanned technologies.

Technologies can be unmanned either because they are only remotely controlled by human actors or because they are not "human" technologies. The last case is the case of the technology addressed by Bonfanti (2014) in his paper. Rigorously speaking, Bonfanti discusses "undogged" rather than "unmanned" technologies, because he is interested in the ethical and privacy issues raised by sniffer devices used in substitution of trained dogs to detect odours. For many years, scent-discriminating dogs have been used by police forces both in criminal investigation and in crime prevention (e.g., drug trafficking, human smuggling, explosive and weapon detection, etc.). Yet humans's best friends present some downsides. They can induce repugnance in some people or be perceived as too physically intrusive, they could also scare children, and, finally, they can hardly witness before a court. In the last decade there has been an increasing interest in developing chemical sniffers, so called "electronic noses". These devises could be used not only for substance detection, but also for human identification. Odour biometrics promise to identify specific odour profiles (odour signatures) which could allow identification and screening of individuals in airports and other monitored environments. Yet odours are full of anthropological and cultural meanings, not to mention their capacity to unravel some

medical conditions including some cancers. So Bonfanti poses himself and to his readers the central question whether electronic noses could be more or less privacy intrusive, and respectful of human dignity, than dogs. An interesting and challenging issue that the author explores is whether, and to what extent, odours can be considered parts of one's own body and whether one could speak of an "odorous space of a person", which is part of his own private, intimate, sphere. Eventually Bonfanti argues that olfactory devices and odour biometrics do not raise novel (or solve old) ethical questions in comparison with dogs, except for the fact that—as it stands—dogs are still more reliable and effective than electronic noses. We are relieved that our best friends are not destined to lose their job in the short period.

Conclusions

In *Political Theology* (Schmitt 1922) Carl Schmitt quotes the young Engels, who wrote "The essence of the state, as that of religion, is mankind's fear of itself". As a psychoanalyst who has worked for years on ethical and societal implications of security, I have found this quotation illuminating. Rephrasing it, one could say that "The essence of security is mankind's fear of itself". Security technologies are theoretically and practically important because they concern the way in which human communities and individuals "metabolise" and manage such a fear.

Insecurity is a constitutive human condition. We are insecure because we live, as Janus, only in the past and in the future, and we ignore the present. Truly, we are always in the middle of an earthquake, although we do not perceive it any longer. Past and future are two abysses, which continuously threaten to swallow us. Catastrophic events are not exceptional; life is made up by, and progresses through, catastrophes, although they often run under our level of awareness. Normality is always, at least in part, fictional as well as our rational understanding of the world. Absurd, non-sense, and violence are always behind the door and threaten to invade in any moment our civilised life. Order in societies—as René Girard has several times argued—is just the fruit of an anterior crisis and a preparation for a future crisis. If technology is always a means to an end, then what other end would be more worth pursuing than providing security?

Acknowledgments I would like to thank the editors of Science and Engineering Ethics, Ray Spier and Stephanie Bird, for having hosted this special issue. In particular a special thanks goes to Ray for his precious suggestions, and to the Springer editorial team, who has put up with my awful delays. A great thanks also to all authors who have contributed to this issue and to all reviewers. Finally I wish to thank Dr. Bruno Turnheim, who has served as an assistant editor, without his dedication this special issue of SEE could have not been possible.

References

Agamben, G. (2013). *Il Mistero del Male*. Bari: Laterza.

Alexander, D. E. (2013). Social media in disaster risk reduction and crisis management. *Science and Engineering Ethics*. doi:10.1007/s11948-013-9502-z.

Annan, K. (1999). Two concepts of sovereignty. *The Economist*, *18*(9), 1999.

Baudrillard, J. (1995). *The gulf war did not take place*. Indianapolis: Indiana University Press.
Bernstein, P. L. (1996). *Against the Gods. The remarkable story of risk*. New York: Wiley.
Bird, S. (2013). Security and privacy: Why privacy matters? *Science and Engineering Ethics, 19*, 669–671.
Bonfanti, M. E. (2014). From sniffer dogs to emerging sniffer devices for airport security: An opportunity to rethink privacy implications? *Science and Engineering Ethics*. doi:10.1007/s11948-014-9528-x.
Büschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y., & Elger, B. (2014). Protecting human health and security in digital Europe: How to deal with the "privacy paradox"? *Science and Engineering Ethics*. doi:10.1007/s11948-013-9511-y.
Buzan, B., Waever, O., & de Wile, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner.
Cacciari, M. (2013). *Il Potere che frena*. Milano: Adelphi.
Capdeville, G. (1973). Les épithètes cultuelles de Janus. Mélanges de l'Ecole française de Rome. *Antiquité, 85*, 395–436.
Cavelty, M. D. (2014). Curing the cyber-in-security paradox with human security. *Science and Engineering Ethics* (this issue).
Colombier, N., Masclet, D., Mirza, D., & Montmarquette, C. (2011). Global security policies against terrorism and the free riding problem: An experimental approach. *Journal of Public Economic Theory, 13*(5), 755–790.
Davis, B. W. (2007). *Heidegger and the will. On the way to Gelassenheit*. Evanston, IL: Northwestern University Press.
Descartes, R. (1989). *Passions of the soul* (V. S., Trad.). Indianapolis: Hackett.
Doyle, B. J. (2009). How (not) to study descartes' regulae. *British Journal for the History of Philosophy, 17*, 3–30.
Ewald, F. (2002). The return of Descartes's malicious demon: An outline of a philosophy of precaution. In T. Baker & J. Simon (Eds.), *Embracing risk. The changing culture of insurance and responsibility* (pp. 273–301). Chicago: The University of Chicago Press.
Fisher, W. (1984). Narration as human communication paradigm: The case of public moral argument. *Communication Monographs, 51*, 1–22.
Foucault, M. (2009). *Security, territory, population: Lectures at the College de France, 1977–1978*. London: Palgrave Macmillan.
Freedman, L. (2004). The new security equation. *Conflict, Security & Development, 4*(3), 245–259.
Giddens, A. (1990). *The consequences of modernity*. Stanford: Stanford University Press.
Glasius, M., & Kaldor, M. (2006). A human security vision for Europe and beyond. In M. Glasius & M. Kaldor (Eds.), *A human security doctrine for Europe: Project, principles, practicalities* (pp. 3–19). London: Routledge.
Hardyn, R. (2013). *The free rider problem*. In E. N. Zalta & A. Cura di (Eds.), *Tratto il giorno May 2014 da The Stanford encyclopedia of philosophy*. http://plato.stanford.edu/archives/spr2013/entries/free-rider/.
Heidegger, M. (1942). *Parmenides* (A. Schuwer & R. Rojcewicz, Trad.). Bloomington: Indiana University Press.
Heidegger, M., & Krell, D. F. (1991). *Nietzsche: Vols. 3 and 4 (Vol. 3: The will to power as knowledge and as metaphysics; Vol. 4: Nihilism)*. New York, London, Glasgow: HarperOne.
Ignatieff, M. (2000). *Virtual war: Kosovo and beyond*. New York: Henry Holt.
Ilchmann, K., & Revill, J. (2013). Chemical and biological weapons in the 'New Wars'. *Science and Engineering Ethics*. doi:10.1007/s11948-013-9479-7.
International Commission on Intervention and State Sovereignty. (2001). *The responsibility to protect*. Ottawa: International Development Research Centre.
ISO/IEC/TMB SAG-Security Secretariat. (2005). *Final report of ISO advisory group on security*. Tratto il giorno January 2014 da International Organization for Standardization: http://www.iso.org/iso/n05_final_report_ags.pdf.
Kreissl, R. (2014). Assessing security technology's impact: Old tools for new problems. *Science and Engineering Ethics*. doi:10.1007/s11948-014-9529-9.
Krieger, H. (2001). *The Kosovo conflict and international law: An analytical documentation 1974–1999*. New York: Cambridge University Press.
Morsink, J. (1999). *The universal declaration of human rights: Origins, drafting, and intent*. Philadelphia: University of Pennsylvania Press.
Negri, A. (1970). *Descartes politico o della ragionevole ideologia*. Milano: Feltrinelli.

Noorman, M. (2013). Responsibility practices and unmanned military technologies. *Science and Engineering Ethics*. doi:10.1007/s11948-013-9484-x.
Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security, 26*(2), 87–102.
Paris, R. (2004). Still an inscrutable concept. *Security Dialogue*, *35*(3), 370–372.
Posner, E., & Vermeule, A. (2007). *Terror in the balance: Security, liberty, and the courts*. Oxford: Oxford University Press.
Radsan, A., & Murphy, R. (2011). Measure twice, shoot once: Higher care for CIA-targeted killing. *University of Illinois Law Review*, *2011*(4), 1201–1241.
Rath, J., Ischi, M., & Perkins, D. (2014). Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. *Science and Engineering Ethics*. doi:10.1007/s11948-014-9519-y.
Rebera, A. P., & Rafalowski, C. (2014). On the spot ethical decision-making in CBRN (chemical, biological, radiological or nuclear event) response. *Science and Engineering Ethics*. doi:10.1007/s11948-014-9520-5.
Schmitt, C. (1922). *Political theology* (University of Chicago Press, 1985 ed.) (G. Schwab, Trad.). Berlin: Duncker & Humblot.
Schmitt, C. (1942). *Land und Meer*. Leipzig: Reclam.
Schmitt, C. (2003). *The nomos of the earth in the international law of the Jus Publicum Europaeum*. New York: Telos.
Schneir, B. (2008). *Schneir on security*. Indianapolis, IN: Wiley.
Sebba, G. (1979). Retroversion and the history of ideas: J.-L. Marion's translation of the regulae of descartes. *Studia Cartesiana, 1*, 145–165.
Shilling, R. (1960). Janus. Le dieu introducteur. Le dieu des passages. *Melanges d'archeologie et d'histoire*, *72*(72), 89–131.
Solove, D. (2011). *Nothing to hide. The false tradeoff between privacy and security*. New Haven: Yale University Press.
Stahl, B. C., Doherty, N. F., Shaw, M., & Janicke, H. (2013). Critical theory as an approach to the ethics of information security. *Science and Engineering Ethics*. doi:10.1007/s11948-013-9496-6.
Study Group on Europe's Security Capabilities. (2004). *A human security doctrine for Europe*. Barcelona: LSE eprint.
UNCHS. (2003). *Human security now*. New York: United Nations.
UNDP. (1994). *Human development report*. New York: United Nations.
United Nations. (2014). *Art.3*. Tratto il giorno May 2014 da United Nations Cyberschoolbus: http://www.un.org/pubs/cyberschoolbus/humanrights/declaration/3.asp.
Virno, P. (2008). *Multitude: Between innovation and negation*. Los Angeles: Semiotext(e).
Zweig, S. (1939–1942). *Die Welt von Gestern* (*The World of yesterday* (Viking Press, 1943 ed.). (A. Bell, Trans.) Stockholm: Bermann-Fischer Verlag AB.