

## View on New and Emerging Security and Surveillance Technologies

Mr. Manjunathraddi J Ajaraddi

Guest Lecturer, RTES Arts, Science, Commerce Degree College, Ranebennur.

### Abstract

While the UN introduced the paradigm of 'human security' in the 1990s, the post 9/11-legislation has returned to the paradigm of national security, in the name of 'homeland' security. The paper explores the ramifications of this reorientation in view of new and emerging security and surveillance technologies. It argues that a culture of surveillance has emerged that contradicts the vision and values of the human security concept. Regarding the intersection of political and private security and surveillance technologies, the ubiquity and entanglement of surveillance technologies with everyday life goes far beyond the purpose of security. Therefore, the paper argues for a reorientation that is backed by moral and political theory, and a (new) social contract that is based on the concept of social freedom, deliberative democracy, and a human rights-oriented concept of justice.

**Keywords:** Surveillance; Deliberative democracy; Human security; Ethics of security; Social freedom

### Introduction

In this paper, I will analyze the recent shift or rather, re-turn in the conceptualization of security, namely from human security as a means to the end of human flourishing, to the new notion of Homeland security under the new conditions of a post 9/11 era. I will limit my investigation to the connection of security and surveillance technologies, the intersection of the political and social applications of these technologies, and the effect of this connection of security and surveillance technologies on the social texture of Northern American and European societies. My reflections stem in part from my work in the ethics committee of the European Commission on ethics in science and new technologies, which, after a year of consultations, hearings and discussions, issued a report on 'The Ethics of Security and Surveillance Technologies' in May 2014 [1] My lecture, however, takes a step back from this report in order to reflect on the specific ethical questions we need to ask from the perspective of a moral philosophy that is rooted in the Christian theological and ethical tradition.

### Human Security versus "Homeland" Security

#### Human security

At the end of the 20th century, the Human Security paradigm was developed as a response to the dissatisfaction with a perspective of 'security' addressing mainly the State whose security should be protected, with the means of military organizations. The 1994 Human Development Report articulated a basic understanding of the function of society, namely to provide basic security for everybody. Deeply related to human development thinking, the new security conception was set from the start to include a fuller picture of human beings than from the limited perspective of violence alone, as present in the traditional security perspective [2]. The report deliberately chose seven areas to broaden the understanding of security: economic security, food security, health security, environmental security, personal security, political security and community security. These were to be conceptualized together, with the individual person being the main addressee. Vulnerabilities and insecurities identify the counter-terms of security, while human flourishing and capabilities serve as the anthropo-ethical telos of development. I would follow Martin, Owen in his proposal to use a threshold approach to human security, building upon the Human Security Commission of 2003: Human security is the protection of the vital core of all human lives from critical and pervasive environmental, economic, food, health, personal and political threats [3] and their report on the human security paradigm from 1994 to

2013, Gasper and Gómez state that organized crime and gang criminality, and not armed conflicts or terrorism, are the major sources of the overall global violent deaths, and hence threats to personal security [4]. Acknowledging the plurality and variety of sources of insecurity in different regions and countries, the human security paradigm aims at contextualizing the sources of insecurity and developing differentiated and new models of interventions.

Human security thinking in general, and work on ‘personal security’ in particular, can be turned into either just a slightly modified continuation of established security thinking related to conflict and crime, or instead be the way through which a fuller picture of humans is introduced and maintained in security-related policies and practices, rendering them more equitable, more relevant and more effective [5].

At the time when the Human Security Paradigm was developed in the 1990s, several armed conflicts occurred that called for a revision of the role of the United Nations. Without a doubt, the wars in Ruanda, in former Yugoslavia, and the Kosovo intervention sparked debates regarding how the role of the international community was to be defined. The so-called *Responsibility to Protect Doctrine* of 2001 [6] is perhaps the last attempt to establish an international framework connecting and combining the human security paradigm and the national sovereignty and national security paradigm. On this level of international discourse, the human security paradigm is acknowledged as the context of the international community’s objectives, when states fail to protect their citizens: 1.28 The concept of human security including concern for human rights, but broader than that in its scope has also become an increasingly important element in international law and international relations, increasingly providing a conceptual framework for international relations.

The Responsibility to Protect Doctrine aims at setting up the principles for international, UN-authorized humanitarian interventions in those cases when states do not act in accordance with the stated responsibility towards the citizens. The UN General Assembly unanimously accepted the doctrine in 2005, however in a much shortened version and a narrower scope (responsibility is defined now as protection against genocide, war crimes, ethnic cleansing, and crimes against humanity).

### **Homeland security**

While the “Responsibility to Protect” 2001 Report was still in the making, the terrorist attack on the World Trade Center changed the perception of US security or insecurity dramatically. In the years following the 9/11 attack, multiple legal provisions passed US Congress that enabled the national (federal) authorities to openly and/or secretly collect information of its citizens as well as of any individual or group, which the quickly re-organized intelligence services considered to be a threat for the US national security. Departing from the broad definition of security the UN still applied within Western societies, the threat to personal security began to reshape the overall perception of insecurity. The Bush Administration now re-framed the security threat in lines of the war on terrorism as a de-localized, de-contextualized global conflict, rendering new ways of warfare necessary and legitimate. Information technologies are key in this strategy to protect US citizens in their security, and surveillance technologies serve as one of the most important means to achieve this goal. The US strategy was more or less copied by other Western countries, however with different emphases depending on the national legislation, economic ability, and perceived insecurity. In fact, it is the intersection of commercial and political surveillance that has resulted in the cultural transformation we currently observe.

One of the most important shifts in the post 9/11 security policy is its pre-emptive or pre-crime nature. We have come to understand the ‘pre-emptive strike’ in the military sector; however, terrorism was so broadly defined that it required and continues to require the surveillance of any social activity. Most importantly, terrorist acts are defined according

to intention rather than action. For example: According to the Patriot Act, computer hacking, carried out from distant computers, is a terrorist act: the enemy is someone with the intention of attacking critical infrastructures information, communications, financial services, energy resources, transport, and distribution irrespective of their geographical or physical location [7]. This de-location of the ‘enemy’ who could attack any part of a given national infrastructure from everywhere is echoed by the de-territorialization of the ‘homeland’ [8]: as security becomes a diffuse concept applicable to all sectors of society, and to all individuals, likewise the “Homeland is no longer definable in terms of territory to defend but a system of values to protect [7].” While US legislation and policy shifted to the new surveillance technology-based ‘Homeland Security’ strategy, it by no means a ‘US’ approach only any longer: In 2006, NATO, already heading the military forces in Afghanistan, adopted the concept of the “Transatlantic Homeland”. Its security practices include not only military intervention, from targeted strikes via drones or other measures to more traditional wars like the one in Afghanistan or Iraq, but also the adoption of emergency laws, spy programs and secret surveillance programs in several countries, with the US, however, being at the center of the transformation. The result of the commodification and privatization of security technologies, going hand in hand with the political authorities’ agenda dedicated to ‘securing the homeland’, is the blurring of several lines previously separated and therefore open to supervision, now becoming more and more intransparent and difficult to oversee. First, the military contracts more and more with, replacing ‘real person analysis’ with computer-based analysis of ‘suspicious behavior’ [12].

private military and security companies [9], which not only act in the shadow of public oversight but, second, also have a high motivation to sell their technologies. Third, the military and police authority tightly collaborate, blurring the lines between these two political authorities. Fourth, commercial data mining and state surveillance programs are no longer separable, as the case of Verizon and the Snowden documents have shown [10]. Fifth, private or civil surveillance technologies and state surveillance programs intersect and interact in public spaces. A thorough analysis of securitization requires interdisciplinary expertise and collaboration not only regarding the technologies involved but also regarding the social, cultural, and economic contexts in particular communities, states, and transnational interactions, as well as the legal and ethical implications.

The re-definition of security as the protection against the enemy by “preemption, deterrence and retaliation” though certainly not uncontested, especially within the European Union where several countries insisted on “regulations, legal and judicial means, and cooperation between civil and police authorities” [11] dramatically alters the human security narrative that the UN established beginning in the 1990s. But it also goes beyond the traditional national security doctrine, because it de-limits the now unilaterally defined and first and foremost ‘securitized’ “responsibility to protect”; it transfers the responsibility to the military, the secret services, and the police who together become the main actors of security, using and in part exploiting the information gathered by civil and/or commercial entities. This shift does not only threaten the human rights based strategy of human security, it also threatens the social contract that is based upon transparency, legitimization of state intrusion into private lives, and the whole range of political human rights most importantly, freedom rights and rights to privacy. Before turning to the cultural and social effects of this shift, let me shortly exemplify what surveillance technologies are used in connection with security issues.

## **The New Culture of Security and Surveillance**

### **Surveillance technologies and security**

Surveillance Technologies are developed in the area of telecommunication, of ICT-based data generated in almost all everyday life practices, from communication to shopping to internet surfing; they also involve, however, areas traditionally thought to be highly sensitive with respect to privacy, such as health-related issues, religious expression,

or political activism. Since surveillance technologies are developed as much in and for civil spheres such as agriculture, ecological monitoring, and public health-related monitoring or emergency aid, as at the same time for the prevention and prosecution of crimes and in the military, they have become ubiquitous.

One of the newer developments where one can observe the blending of contexts concerns biometrics and other body monitoring systems, and so-called ambient intelligence technologies: embedded software, ubiquitous computing, smart objects, and the ‘internet of things’ all point into the direction of object-subject interactions through the human body. In the near future, for example, the traditional CCTV video camera surveillance of public spaces will be replaced by dynamic video analytics, replacing ‘real person analysis’ with computer-based analysis of ‘suspicious behavior’ [12].

By using these technologies or by being subjected to identification measures, we constantly produce data that may or may not be collected, sorted through, and stored. The registration, identification and authentication of devices result in the availability of data on movement, behavior, location etc., potentially communicated to and stored in central databases. Private companies as well as state authorities as we have come to know over the last few years make increasing and extensive use of these data, either to predict commercial behavior, or behavior that may be relevant for security issues. Not only are devices and software shared between the private sector and political bodies, it is also the case that many employees of the private sector transfer to the political and vice versa over the time of their career. Cameras, radio frequency identification (RFID), or wireless sensors already now collect bodily functions such as facial expressions or eye movement, for example at airports or during big public events; biometrical data concerning age, gender, ethnicity, or body weight, combined with specific bodily functions such as pulse or body temperature may be traced in specific environments, e.g. particular working places. Beyond political surveillance, body-monitoring sensors may, for example, be used to ensure safe living conditions for the elderly, potentially applied as body implants. It is no longer privacy only that is affected but also bodily integrity, and this technological development certainly radicalizes what Foucault [13] called ‘biopower’: it is not just controlled from a governmental authority but takes on multiple forms, it is embodied by everyone, and all the information cannot be controlled any longer by oversight institutions: even for the supervision of the surveillance technologies, we have become dependent on specific software programs and experts who may or may not release the information they have to the public, or to the democratically elected political authorities.

The EGE summarizes the characteristics of the new surveillance technologies under the headings of *miniaturization, ubiquity, automation, integration and convergence of technologies*. Summing up the descriptive survey of the different kinds of surveillance technologies, the EGE concludes: Deployment of security and surveillance technologies, irrespective of their origins, was once considered the prerogative of the State or its agencies. This is no longer the case with commercial entities and individuals utilizing technologies which allow them to survey their customers and neighbours and draw inferences about future behavior from past actions. Much of this technology is transformative and offers concrete benefits to individuals and larger society. Reaping these benefits are however dependent upon the proven effectiveness of the technology and its proportionate use [1].

The last two criteria, effectiveness and proportionality, must be complemented with transparency and accountability with respect to the overall legal frameworks. Oversight, however, has become more and more difficult. The EGE examining the security and surveillance technologies of the EU alone saw many legal loopholes, mostly stemming from the fragmented regulatory instruments.

Given, however, the intersection between commercial and political interests, the so-called ‘push/pull’ dynamic requires comparative analyses between technologies (as well as between new technologies and other means of protecting the security of citizens), and it requires the critical analysis of the market interests of security companies.



## Surveillance society

As I have argued above, the technological developments are often driven by the reorientation of the security paradigm; their increased applications were intensified, however, by the exploitation of the very same technologies by companies to predict the commercial behavior of customers. In the following, I will extend my perspective to the cultural analysis. It may not be exaggerated to state that both the American and European societies have transformed their own vision of the 'liberal society', based on democracy, separation of powers, rule of law, and free, peaceful, and tolerant social cooperation, to the vision of an ever- services and criminal justice; our health and well-being and our movement through public and private spaces [14].

According to this definition more homogenized society that must protect itself against the 'other' threatening 'our' way of life, potentially making use of 'exceptional means', namely means that do not comply with the rules of democratic states or even given legislation. When surveillance technologies are combined with a particular security paradigm that I have defined as "Homeland" Security, specific 'others' need to be identified, both within the societies as well as outside of it.

Security, in this vision, creates or co-creates a particular collective identity, a value system and a virtual 'land', the "homeland", to which only those belong who share its unquestioned and unquestionable values. Surveillance technologies are only one group within the broad field of security technologies required to defend these values: at first sight, they seem to resemble traditional civil systems, like locks or alarm systems to secure one's property, especially the things we use while moving in the public sphere: cars, bikes, cell-phones, laptops, credit cards, etc. They also seem to resemble newer security systems aimed at protecting our transactions, social communication and cooperation in cyberspace all of those already a response to the 20th century social transformations of our daily lives. Since some of the same security technologies, however, are also used as part of police and military equipment, the lines between the civil and the state security systems are constantly blurred. Resistance is all the more difficult as the new technologies are readily embraced by civil society, eager to profit from the new ICT developments. Surveillance technologies, as they have emerged over the last decades, however, play a decisive role in the transformation of our culture that goes beyond the daily care for security we have all internalized, albeit most probably without understanding how much of our private data is collected and stored. In their report on the "Surveillance Society" from 2006, Kirstie Ball and David Wood define this transformation in these words: The surveillance society is a society which is organised and structured using surveillance-based techniques. To be under surveillance means having information about one's movements and activities recorded by technologies, on behalf of the organisations and governments that structure our society. This information is then sorted, sifted and categorised, and used as a basis for decisions which affect our life chances. Such decisions concern our entitlement and access to benefits, work, products and , information may be collected and used by private and commercial organizations as well as by governments; we may consent or not, we may know or not know who uses what information for what purpose with what authority and yet, information is collected with purpose, routinely, systematically, and focused (Ball/Wood), 'sorted, sifted and categorized, and used as a basis for decisions which affect our life chances', mostly without citizens' or public deliberation or participation.

Surveillance of all, however, creates a tension within the framework of security: it does not discriminate between those who may threaten the security and those who just live with the fact that they are surveilled. Going through the airport security, for example, we know and must consent in order to fly that multiple personal data are collected and screened. We also have become used to body scans, even though we do not exactly know how they work, what information is gathered, what safety risks are involved, or even what the employees of the TSA see or do while we are scanned [15]. Yet, we trust that we belong to the group who is either targeted in a positive way in the US, this means becoming global entry customers, for example

or at least not targeted in a negative way by the ‘system’: we are the ‘good’, we are ‘we’, and not the ‘others’ the others who threaten us in our security and identity, in are the ‘good’, we are ‘we’, and not the ‘others’ the others who threaten us in our security and identity, in our way of life, or who even threaten our very life in a situation, as a flight certainly is, of increased dependency and vulnerability. Hence, we not only comply with the rules of indiscriminate surveillance, we also explicitly or implicitly comply with discrimination, on the basis of the social construction of the ‘other’ all based upon real or constructed threats that we ourselves cannot judge, let alone compare or assess in comparison to other threats to our security it is here that the priority of personal security over against human security is assumed but not openly discussed, because the measures of surveillance are not accessible; this has ethical ramifications, but these are no longer publicly debated or debatable, because any public reasoning takes place in the wake of the images and experiences of terror attacks. Security measures, it seems, are almost entirely constructed and perceived as ‘our’ response to ‘Islamistic terror’. It is not necessary for this cultural transformation that we – the citizens of nation states or the European Union, for example – have a fixed understanding of the ‘we’ and the ‘others’; rather, a certain collective identity is formed by design: by the technologies and practices of surveillance, each of which possibly sensible and not “a big deal”, but taken together creating new norms of the good or bad citizen. In other words: in the name of security, social sorting is built into the security and surveillance technologies: Governmental logic has changed. While older, twentieth century understandings of citizenship stressed the inclusion of all eligible persons in systems of health, welfare and legal protection, newer citizenship practices, including ID systems, seem to stress exclusion of undesirable elements [16]. Those with access to resources are highly mobile. But for others, who are working (or worse, unemployed) migrants, refugees or asylum seekers, not to mention those with distinctive ‘Muslim’ or ‘Arab’ names, these systems tend to militate against movement both within and between countries [14].

The indiscriminate surveillance, for example in the closed circuit television (CCTV) cameras used in public spaces, monitoring all movements, and the social sorting embedded in the use of the data gathered, creates a tension between security and personal insecurity: the individuals who are recognized as belonging to the ‘we’ may feel secure when they are monitored in the UK, for example, almost 5 million CCTV cameras are used, equated one camera for every 14 people but citizens are constantly at risk of losing exactly this social status, especially when the criteria for the ‘othering’ are not made transparent. It is this fear of becoming the other, and as such becoming the ‘target’ of ‘negative’ surveillance, that feeds into the normalization of one’s behavior. Control starts with the control of oneself, a phenomenon that Foucault has described as biopower or disciplining of one’s behavior. Security measures are therefore not only a response to an objective and/or perceived insecurity; they also create another kind of insecurity that becomes part of the individual and collective identity: I may be considered as a suspicious person in the eye of others (or an anonymous system created by designers of algorithms, according to the tasks given to them) and I may consider others with pre-judiced concepts that have been shaped and are constantly shaped by the images of the other, through cultural, social, and political mediations.

In a culture of security and surveillance, the trust that is necessary for any social cooperation and interaction easily erodes between individuals, within communities, between citizens and the state, and even between the international actors. But it is the intersection of the social and commercial security with the political paradigm of ‘homeland’ security, re-emerged since the beginning of the 21st century, that takes the culture of security to another level. I agree with David Garland who has coined the term culture of control with view on the criminal system in the US: This culture materializes in part as a culture of security and surveillance, based upon the ‘othering’ of particular individuals and groups. It is this ‘othering’ that renders the ‘homeland’ security paradigm a threat to democracy.

## Conclusion:

Reorientation of the Security Paradigm: Christian Ethics and the Ethics of Security This development must be a concern for any ethics. Since Thomas Hobbes' *Leviathan*, security has been regarded as the decisive motivating force for individuals to consent to the *contrat sociale*, giving up some freedoms (especially the freedom to defend oneself against another, in order to preserve one's life) and gaining the security that renders a social life of peace and cooperation with others possible. Hobbes' view the 'trade-off' between liberty and security in the social contract however, marks only the beginning of modern political philosophy. Hobbes' version of the trade-off between security and liberty is not based on a moral theory of freedom and well-being as it is articulated in modern theories of human rights. It reflects a highly hierarchical social and political order that precedes the later vision of granting everyone equal rights, beginning with the political rights, and further developed over the last two centuries as civil rights, and then as social, cultural and economic rights.

Although I cannot pursue the history of the relation of freedom/ liberty and security here [17], we must note that both ideas of human rights and democracy have transformed, among other things, the social contract. Security is not the only motive for individuals to 'socialize' or to affirm a specific form of political government: if we take, for example, 20th century social psychology and philosophy resting on Hegelian philosophy as one alternative concept, then according to this model, individuals are necessarily 'social selves', capable not only of pursuing their interests while fearing the intervention of others into their 'individual freedom zone' but also capable of taking their perspectives, needs, and desires as positive motivation for their own actions. The desire to 'have and lead a good life with and for others in just institutions', to recall Paul Ricoeur's famous definition [18], becomes the motivational centerpiece of an ethics that is radically different from the Hobbesian view on the moral selves, complemented by the normative perspectives that connects one's rights with one's duties to respect oneself and the other, to care for oneself and the other, and to establish, critique, or reform institutions, when they do not reflect the responsibility to protect the basic, civil, and social human rights of all human beings. Being constituted by social realities, contexts, communities, and personal relations, individuals come to learn to interact and participate socially via taking the perspective of the 'other', relating and comparing it with their own interests and interpretations of reality. They learn to engage in practices almost always together with others, and they learn how they co-construct the very architecture of governing that at the same time shapes certain parts of their identity, in a dialectical movement of construction, critical correlation, and correction. Part of their agency, however, concerns moral agency that is based upon the very reflection on why one must respect and care for the other. It is true that the Kantian or Neo-Kantian moral theory of human dignity and human rights is a normative concept and not the representation of lived political practices; and given the current state of affairs, it is not uncontested even on this level of normative theories. And yet, its vision is that individual ethical desires and interests, namely to live with and for others in just institutions, match and must match with the normative frameworks and institutions that enable individual flourishing and social cooperation. The two perspectives together the ethical perspective of the individuals or groups of people who share a common history and/or vision, and the moral perspective of institutions who are founded on every agent's yearning for freedom and well-being, create or contribute to the social freedom and security that is embraced rather by the human security doctrine than by the ideology of the homeland. Axel Honneth [19] has recently introduced the term of social freedom (over against the Hobbesian negative freedom and the Kantian reflective freedom), in order to capture the modern form of freedom that is based on mutual recognition of the self and the other in personal relations, in social interactions, both granted and secured in the political and legal system of the state [20,21]. This concept, together with the theory of deliberative democracy can be used as a jumpstart for the development of a security ethics that is based on social cooperation and mutual recognition, grounded in the modern concept of human rights, including but also

going further than the political freedom rights of every individual, and the political responsibility to secure and protect all of these rights of all people.

Governance driven by fear, in contrast, divides the world into friends and foes; it may be legal, but it is disconnected from justice that grants everybody equality before the law. Furthermore and as important on the cultural level, it keeps individuals and collectives from seeing each other as a neighbors. Neighbors are neither friends nor foes; they have not chosen to be together, and yet they can and in fact must share the world they live in. While there is every reason to be diligent and responsible in view of threats to anybody's security threats that are and must be empirically analyzed, making at least in part use of surveillance measures and while there is every reason for any ethics theory to deal with the problem of violence and crime, fear of one's neighbor is a bad precept for social cooperation. Instead, it creates just another kind of insecurity. Finally, and perhaps most importantly for the task of today's moral philosophy, fear used as political ideology keeps us from asking critical questions concerning the underlying agenda of the political security paradigm. This easily ignores that transnational and international cooperation is badly needed on a political level, in order to secure the human rights and well-being of all people, with billions of them vulnerable to basic insecurities, captured in the threshold definition of the human security paradigm. But it also ignores that recognition goes far beyond the political. Security ethics that is spelled out as ethics of recognition and responsibility will scrutinize our practices in different social settings and contexts, in order to find new ways of social cooperation for example, between religious communities, youth initiatives, family programs, or even corporate social identity measures, etc.

There can be no question that terrorist attacks such as the ones the world witnessed on September 11, 2001 in the US, and continues to witness both nationally and internationally until today, cannot be tolerated by any society, and certainly not by the international community. Likewise, the world community cannot and must not stand by when groups exploit religions as an ideology for committing crimes, among them crimes against humanity, which would be covered by the "Responsibility to Protect" Doctrine. However, surveillance in its current scope and application is neither effective nor prudent nor ethically sound. Instead, the broader Responsibility to Protect Doctrine that the UN developed at the turn of the Millennium must serve as an orientation for a realistic political ethics, one that Christian ethics, too, may be able to embrace and develop further as a normative framework. This, however, is only possible if it is redirected to the broader framework of human security, and if responsibility is linked to accountability for any political action or omission, including those of the international community.

Hence, it is our task, first, to analyze the connection of security and surveillance technologies as reflection of a particular concept of security, and second, to criticize its contradiction of the unfinished transformation of the social contract based on human rights and human security. Third, rather than 'trading off' one's liberties and freedom for the good of security, we need to understand that security necessarily entails and promotes the freedom of those whose lives are secured. It is for this reason that surveillance technologies require transparency and supervision and all states need to set up procedures to ensure that this is possible. Finally, drawing to my own tradition, namely Christian ethics, fourth, ethics must not only confront the new culture with its own normative principles of the love of neighbor (spelled out as responsibility to care), the dignity of every person, solidarity and the common good, but also with the principle of justice, calling for the re-ordering of priorities in international policies. In part, the ethics of justice calls for the justification of how money is spent, for what, in the name of whom, and for what purposes.

Ultimately, however, ethics will also need to be clear: life cannot be secured by any means, and violence and crime will always be part of human history. While ethics cannot and must not shy away from the truth that vulnerability is part of the human condition, it must still speak out against violence and crime. And yet: it is not fear but care for the other that enables



us to respond responsibly to those with whom we share the world we live in. Recognition of our own dignity expresses itself in our capability to recognition the other as someone whose wellbeing is indeed our responsibility.

## References

1. European Group on Ethics in Science and New Technologies (2014) Ethics of Security and Surveillance Technologies. European Commission, Brussels.
2. Gasper D, Oscar AG (2014) Human Security–Twenty Years On.
3. Owen T (2014) Human security thresholds. In: Mary M, Owen T (ed) The Routledge Handbook of Human Security. Routledge, London/New York.
4. Fiona R (2011) The ethics of care: a feminist approach to human security. Temple University Press, Philadelphia.
5. World Health Organization (2013) Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence. World Health Organization, Geneva.
6. Gasper D, Oscar AG (2014) Evolution of Thinking and Research on Human and Personal Security 1994-2013. UNDP Human Development Report Office, Occasional Paper.
7. International Commission on Intervention and State Sovereignty (2001) The Responsibility to Protect. Ottawa.
8. Gygas J (2010) Strategic culture and security. American antiterrorist policy and the use of soft power after 9/11. In: Basil G, Hanhimaeki J, Soutou GH (ed) The Routledge Handbook of Transatlantic Security, Routledge, London/New York: 231-249.
9. Mattea K, Chris H (2013) Homeland Security: The Trillion-Dollar Concept That No One Can Define. TomDispatch.com.
10. James P (2014) The morality of private war: the challenge of private military and security companies. Oxford University Press.
11. Landau S (2011) Surveillance or Security? The Risks Posed by New Wiretapping Technologies. MIT Press, Cambridge/MA.
12. Vincent P (2010) International Security in Practice: The politics of NATO/Russia diplomacy. In: Christian RS, Nicholas JW (Ed) Cambridge Studies in International Relations 113. Cambridge University Press, Cambridge/MA.
13. Keith P (2013) The great surveillance boom. Fortune.
14. Michel F (2007) Security, territory, population: lectures at the College de France, 1977-78. Palgrave Macmillan, Basingstoke/New York.
15. Kirstie B, David MW (2006) A Report on the Surveillance Society.
16. Edward H (2014) Dear America, I saw you naked. Politico.
17. Bigo D (2004) Globalized in-security: the field of the professionals of unease management and the ban-opticon. Traces 4.
18. Conor G (2013) Liberty and Security. Polity Press, Cambridge.
19. Ricoeur P (1992) Oneself as another. University of Chicago Press, Chicago.
20. Honneth A (2011) Das Recht der Freiheit. Grundriss einer demokratischen Sittlichkeit. Frankfurt suhrkamp.
21. Honneth A (2014) Freedom's Right. The Social Foundations of Democratic Life. Columbia University Press, New York.