Putting critique to work: Ethics in EU security research

Matthias Leese
ETH Zurich, Switzerland

Kristoffer Lidén
Peace Research Institute Oslo (PRIO), Norway

Blagovesta Nikolova
Bulgarian Academy of Sciences, Bulgaria

Abstract
In this article, we examine the possibility of exercising critique through the mandatory ethical coverage that EU security research projects must be subjected to. Applied ethics, so we argue, speaks to several core issues in the critical security studies agenda, such as turning abstract considerations of critique into forms of tangible cooperation, engaging exoteric communities, and placing normative questions about security within concrete contexts of its imagination and production. Accordingly, it can be seen as a concrete way of putting critique to work. At the same time, however, applied ethics does face considerable challenges that result from its location in the middle of numerous cross-pressures, such as political ambitions, economic interests, technological rationales and the demands of security professionals. These challenges risk turning what was intended to be the critical corrective of applied ethics into a legitimizing function of mere 'ethics approval'. Drawing on personal experiences as well as debates on critical security studies and ethics, we discuss some of these challenges and discuss the possibility of and conditions for critique within the arena of EU security research.

Keywords
Critique, ethics, European Union, security research, technology

Introduction

> In the popular imagination, in the world of technology and scientific innovation, and in the contemporary political arena, in every newspaper and newsmagazine, phrases like 'ethical responsibility' (and 'ethical lapse') appear with startling frequency. Whether it's the sex scandal in the White House, the debate about human cloning, or the question of campaign funding reform, we have become inured to the idea that 'ethics' is a kind of moral orthopedics. (Garber et al., 2000: vii–viii)

Corresponding author:
Matthias Leese, ETH Zurich, Haldeneggsteig 4, IFW, Zurich, 8092, Switzerland.
Email: matthias.leese@sipo.gess.ethz.ch

What Garber et al. (2000) have deemed 'the turn to ethics' is no stranger to the study of security. Critical scholars have foregrounded how security is tied to contested values, and how it 'articulates particular understandings of our relation to nature, other human beings and the self' (Huysmans, 1998: 228). Subsequently, it has been argued that the critical security studies agenda should always bear in mind ethical questions when engaging with the conditions and effects of security (e.g. Bigo, 2002; Booth, 1991; Browning and McDonald, 2013; c.a.s.e. collective, 2006; Der Derian, 1995; Huysmans, 1998). Ethics, however, is not limited to conceptual reflections about security and its status in society and politics, but can also serve as a practical angle for engaging the ways in which security is imagined and produced. Such an angle is particularly pertinent vis-a-vis research and development activities. As Haggerty (2004: 392) points out, 'concerns about the ethical quality of research are characteristic of a society where anxieties about the unintended consequences of science and technology are increasingly common'. Research programmes, and specifically those that receive public funding, therefore need to comply with ethical obligations.

Through its Framework Programmes (FPs, the current one being 'Horizon 2020'), the European Union spends increasingly large amounts of money (the budget for the 'Secure Societies' theme from 2014 to 2020 is close to 1.7 billion euro)[1] on research projects that seek in one way or another to contribute to 'protecting [the] freedom and security of Europe and its citizens'.[2] This contribution is primarily seen as 'producing new and improved technologies and security solutions to strengthen practitioner capabilities and the competitiveness of the European security industry' (Protection and Security Advisory Group, 2016: 2). As security technologies have, however, proven to be prone to unfolding negative repercussions and undercutting human rights and civil liberties (e.g. the rights to privacy and data protection, non-discrimination, and inclusion), or to reproducing and reinforcing power imbalances and social injustice (see, for example, Burgess, 2012, 2014; European Group on Ethics in Science and New Technologies to the European Commission, 2014; Hayes, 2006), EU-funded research must now be accompanied by applied ethics (i.e. the study of normative issues in concrete contexts) that analyses the normative implications of the project activities during the funding period.[3]

Ethics is thus politically perceived as a way of providing normative guidance that speaks to a recognition of the ambiguous nature of security, and is supposed to nudge research in a normatively desirable direction (see, for example, European Commission, 2013, 2015). Most importantly, it is supposed to actively engage the involved stakeholders in security research, including the likes of policymakers, industrial companies, researchers from technical disciplines (e.g. engineering, computer science) and so-called end-users (e.g. police agencies, emergency planners, blue-light services and other security professionals). In critical security studies, such engagement with the 'exoteric communities' that are involved in the imagination and production of security has been flagged by the c.a.s.e. collective (2006: 473) as a key task vis-a-vis the question of how to possibly translate critique into tangible political and practical prescription – a question that has sparked continuous controversy within the field since its early days (Hynek and Chandler, 2013).

If, as Bigo (2002: 64) argues, 'critique reinforces the vision of a contest between ideas and norms', and this is 'a contest in which academics can play a leading role', then questions of how this role could be practically exercised are pertinent for an academic field that deems itself 'critical'. We engage such questions here through the role of applied ethics in EU security research projects. We claim that the diverse practices of such 'accompanying' ethics work (e.g. establishing a dialogue with technical partners and raising awareness of ethical stakes; providing input to technical components and processes; developing best practice guidelines or evaluation schemes for project components) offer a potential way to 'put critique to work' and address the common reproach that critical security studies would all too often stop at a deconstructive notion of critique without offering viable practical alternatives. We do, however, at

the same time seek to draw attention to the challenges that applied ethics faces vis-a-vis the organizational structure of EU security research projects, the agendas and perceptions of involved exoteric communities (e.g. the economic interests of industry, the practical perspectives and requirements of end-users), and the risk of legitimizing problematic research and development activities through one's very participation.

The article proceeds as follows. First, we review the scope for ethics in the critical security studies literature. We then describe how ethics becomes incorporated into EU security research projects as a monitoring and guidance tool. Eventually, we discuss the multiple challenges that critique in the form of applied ethics is subjected to in everyday security research, and suggest what the preconditions for addressing these challenges are, in line with our observations on the perils and prospects of political prescription in critical security studies.

Methodological note

The analytical part of this article is not based on empirical research in a formalized sense. It is, however, based on multiple years of professional expertise as ethicists in EU security research projects that we share among us. It thus presents a personalized account of the challenges that we encountered in our work, which are not necessarily representative. Our experiences, however, have been confirmed by many of our colleagues in similar roles, both in informal exchanges and in more formal frameworks (e.g. workshops and conference panels). Examples and quotes from project documents and personal notes throughout the article have been anonymized.

Security, critique, ethics

The conceptual relationship between security and critique remains a contested one in critical security studies, despite an already vast and growing literature on the subject (e.g. Booth, 2005; c.a.s.e. collective, 2006; Fierke, 2007; Hynek and Chandler, 2013; Krause and Williams, 1997). More than 20 years ago, and vis-a-vis the 'development of a self-consciously critical perspective within security studies', Williams and Krause (1997: vii) posited the need to move away from a hitherto-prevalent problem-solving, policy-oriented self-understanding of security studies, and towards a more reflexively informed approach that interrogates the meaning of security rather than taking it for granted. Huysmans (1998: 244) has in this vein suggested understanding security as an 'ordering activity' that 'arranges social relations in a particular way', thus drawing attention to the normative societal repercussions of security politics and practices. The 'critical' element in critical security studies could in this vein be broken down to careful scrutiny of such politics and practices, aiming to expose their underlying assumptions, rationales and stakes in order to uncover how and for what purposes security is shaped and enacted (see, for example, Hutchings, 2001; Jabri, 2016).

Geared towards analyses of how power operates in the construction and government of security issues, such a reading of critique, however, has at times been accused of favouring deconstructive forms of analysis and stopping short of offering productive alternatives. As Nunes (2012: 348) points out in this regard, 'while critical security studies has been successful in contesting predominant security arrangements, its achievements when it comes to providing a normative agenda and informing political change are arguably more modest'. Pertinent in this context is Hynek and Chandler's (2013) claim that critical security studies has during the past two decades failed to live up to its critical theory roots and has not managed to offer convincing emancipatory alternatives to the political order under study. For Williams and Krause (1997), it has indeed been clear early on that any deconstructive notions implied by a critique of security on a conceptual or practical level would need to be productively reconstructed. As they argue, 'if a critical theory involves

de-essentializing and deconstructing prevailing claims about security, then the question of how security is redefined seems necessarily to follow' (Williams and Krause, 1997: xiv). The answers to this question, however, have been anything but unanimous.

Whereas for critical theorists, the modus operandi for critique must come in the shape of emancipatory alternatives, others have suggested conceptualizing critique through a reading of the very notion of security itself as an ethical category. Conceiving of security as a value or common good would thereby render its study in terms of normative debates (see, for example, Burgess, 2011b; Burke, 2013; Nyman and Burke, 2016a). Nyman and Burke (2016b: 3) have in this sense argued that ethics is a fundamental yet undertheorized part of academic engagements with security, and that 'there is a need … for ethical principles and reasoning to be deployed in both the critique and advocacy of various norms and social practices'. Such an approach to security and critique is, however, in itself not unproblematic, as it arguably presupposes the normative as a given category instead of something that must equally be subjected to challenge and contestation (Sjoberg, 2013). Moreover, conceiving of security as ethics would risk reinforcing the mobilization of security as a means of power that to a large extent sparked the emergence of critical security studies in the first place. As Jabri (2016: 27) summarizes this quandary, 'the point at which security is transformed into a universal ethical category is also the point at which it becomes a technology of domination, of the governing over the governed'.

One must at this point be careful not to conflate distinct readings of ethics when it comes to critical analyses of security. Whereas the position advertised by Nyman and Burke conceives of security *as* ethics, a different vantage point emerges from ethical reflection that focuses on the normative effects of security politics and practices across society (e.g. Bigo, 2002; Browning and McDonald, 2013; c.a.s.e. collective, 2006; Der Derian, 1995; Huysmans, 1998). Understood in this sense as ethics *of* security, Browning and McDonald (2013) identify the search for 'good security' as a key concern for critical security studies. While they in fact do problematize the hegemonic struggles that result from competitive visions about what such good security would entail, who would be in a position to make judgments about the quality of security, and how the notion of good security could be located among notions of resistance, emancipation or desecuritization, they conceive of ethics as an unsettling and reflexive element that, in the vein of 'doing critique' and challenging established positions and knowledges, can help to problematize the ways in which security is enacted.

Such a notion of applied ethics, understood as 'deliberation about values with reference to praxis' (Flyvbjerg, 2001: 57), can indeed critically inform academic engagements with security politics and practices and help to convey critique. Moreover, applied ethics speaks closely to the practice orientation of the critical security studies agenda, as it has the capacity to provide 'input to the ongoing social dialogue about the problems and risks we face and how things may be done differently' (Flyvbjerg, 2001: 61). The notion of dialogue is important here. Claiming that 'there is no clear boundary between the practices of theorizing security and practising security', the c.a.s.e. collective (2006: 473) has put forward that critical scholars must not remain in the academic ivory tower, but should rather be willing to engage with communities of practitioners and become actively involved in the ways in which security is imagined and practised. In this sense, the members of the collective have argued that 'the most direct contribution of [critical security studies] lies in its attempts to assist security practitioners in becoming more reflexive about their practices, as well as in helping them to cope with multiple truths, theories and technical knowledge' (c.a.s.e. collective, 2006: 474).

We believe that security research programmes offer a pertinent opportunity to do just this. Bigo et al. (2014: 9), with specific reference to EU security research, have argued that 'technological tools and services cannot be developed without a thorough legal, social and political assessment',

and that social science should 'be conceived as a specific research priority with its own agenda, informing more technology and industry-focused programmes'. We endorse such a pragmatic stance that is context dependent and oriented towards action, and argue that security research opens up a concrete way of practising critique, as it presents us with an arena in which 'security' and 'ethics' take on concrete and tangible forms through interaction between academics, security professionals, policymakers and industry. Applied ethics in this context provides a unique possibility to both analyse and engage security in the early stages of its imagination and production. Ethics should in this vein not be misunderstood as a theorization of security itself, but rather understood as a *practical angle* of engagement with the world and the workings of security within it.

Rather than reducing the relationship between security and critique to theoretical considerations, applied ethics thereby allows us to maintain a focus on the concrete politics and practices of security as they emerge in the arena of security research programmes. The invocation of applied ethics should therefore not be understood as an attempt to theorize critique in novel terms vis-a-vis conceptual debates about security, but rather as an instrument to 'put critique to work' that allows us to bridge the gap between academic reflexivity and practical engagement. At the same time, while not going as far as offering radical emancipatory alternatives outside of the existing sociopolitical system, applied ethics provides for a break with 'a radical understanding of critique as the permanent questioning of security' (Nunes, 2012: 348), and instead forces critical scholars to channel normative critique into tangible policies, best practice guidelines or technologies. We in this sense conceive of critique and applied ethics as closely entwined elements that can help to productively recharge the critical security studies agenda.

The role of ethics in EU security research offers an example through which these dynamics can be studied. On the one hand, the inclusion of ethics holds the promise of aligning security research and development with principles like human rights and democracy – instead of quelling these in the name of security. On the other hand, it reinforces the political legitimacy of the research projects without necessarily fulfilling their ethical promises in practice. Even when it is allowed into the realms of power where technologies and strategies of security are developed – with adequate funding and formal mandates – a series of organizational and normative constraints associated with 'power' in critical security studies risk forcing ethics into the folds of hegemonic practice (Hynek and Chandler, 2013). This brings us to an investigation of the promises and practical constraints of fulfilling the formal role of ethics in EU security research and of the potential for overcoming the constraints through pragmatic engagement.

Ethics and EU security research

Security research activities funded by the EU have over the past years increasingly commanded ethical attention. This increased attention must be read against the backdrop of a technologized and market-oriented vision of security production (see, for example, De Goede, 2011; Hoijtink, 2014) and the political recognition that there is no such thing as innocent scientific or technological progress. On the contrary, as Haggerty (2004: 392) notes, 'where modernity manifests a general trust in the ability of science to resolve our most pressing problems, we have become attuned to the truth that science itself poses risks and that these risks can no longer be explained away as temporary aberrations in the march of progress'. Issues such as large-scale surveillance, infringements of privacy and data protection, profiling, or discrimination have generated increased public attention towards security technologies under development (see, for example, Burgess, 2014; Leese, 2017; Valkenburg, 2017), and multiple studies for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs have argued that EU security research projects should show stronger concern for ethical implications of the products

under development (Bigo et al., 2014; Jeandesboz and Ragazzi, 2010). Politically, stronger incorporation of ethics into security research can be seen as a strategy for addressing these issues, and this has become particularly apparent with Horizon 2020 and its reinforced attention towards the possible societal ramifications of technological change.[4]

The thrust towards ethics must arguably also be read vis-a-vis the self-identification of the EU as a 'community of values'. With the Treaty of Lisbon (*Official Journal of the European Union*, 2007), the Charter of Fundamental Rights of the European Union (European Union, 2000) became a main point of reference not only for EU policymaking in general but also with specific regard to ethical principles in research and development activities. Compliance with 'fundamental ethical principles', promoted for the first time in FP5 (*Official Journal of the European Communities*, 1998), has since become legally binding and corresponds closely with the EU agenda on Responsible Research and Innovation (RRI) that highlights wider ethical and societal aspects of research (European Commission, 2012c, 2013). RRI foregrounds notions of participation, reflexivity, deliberation, anticipation, social justice and value-sensitive design in research (see, for example, Grunwald, 2014; Owen et al., 2012, 2013; Von Schomberg, 2011), and is considered a viable instrument to 'achieve a better alignment of [research and innovation] programmes and agendas with societal needs and concerns' (European Commission, 2015: 9).

In Horizon 2020, Article 14 of the Rules for Participation (*Official Journal of the European Union*, 2013) specifies a systematic ethics review for all grant applications. The first stage of this consists of a so-called ethics self-assessment to be carried out by the applicant (i.e. the project consortium). During the assessment, consortia are expected to refer to a number of already predefined 'ethics issues' (including the likes of human embryos and foetuses, human cells or tissues, and animals, but also personal data, dual use, exclusive focus on civil applications and potential misuse of research results) and indicate whether these issues could become relevant during the proposed research (European Commission, 2016). Especially the latter categories are pertinent for security research, as many projects involve some form of data collection that falls under the scope of data protection law, and basic technologies could have military applications or developed tools could be misused to inflict harm. In one of our projects, for example, interviews with practitioners were conducted in order to map the practical application contexts for the technological tool under development. Per the ethics self-assessment, this albeit rather common way of surveying end-user requirements did raise data protection concerns. And in another project, the development of a multichannel alerting tool for disaster management triggered the 'misuse' category, as the tool could potentially be used to distribute inaccurate or misleading information and therefore infringe the autonomy of individuals.

Thus, there is a high likelihood that for proposed security research projects one or more relevant categories will apply, and when this is the case, project consortia are expected to include a dedicated ethics section in the grant proposal that demonstrates awareness of potential wider societal repercussions of the project goals and specifies the ways in which the project plans to deal with the issues identified. The Commission guidance document on 'How To Complete Your Ethics Self-Assessment' (European Commission, 2016: n.p.) in this vein explicitly encourages applicants to address ethics issues already in the design of their project, and reminds applicants that 'ethics issues arise in many areas of research' and that 'you must protect your volunteers, yourself and your researcher colleagues'.

Practical hints about how to do so are provided in the European Commission blueprint grant agreement (European Commission, 2017a) that includes a section on ethics questions (Article 34) and specifically references the European Code of Conduct for Research Integrity (ALLEA,

2017), with its emphasis on the principles of reliability, honesty, respect and accountability in research. A second point of reference is provided by the EU's RRI framework (European Commission, 2017b). A report from the Expert Group on the State of Art in Europe on Responsible Research and Innovation had in 2013 already suggested 'to mainstream RRI in the existing funding programmes' (European Commission, 2013: 26), and this was supported by a more formalized study on how RRI could serve as a framework for monitoring research and development activities (European Commission, 2015). The study put forward that 'ethics is one of the RRI criteria in greatest need of new concepts and designs for indicators' (European Commission, 2015: 34) and proposed specific instruments to ensure that research outcomes are ethically acceptable, including a 'documentation regarding normative tensions related to research integrity policies and actions' and an 'ELSI/ELSA project component for ethical acceptability' (European Commission, 2015: 36).[5]

These elements now become legally binding parts of EU security research projects when, during the second stage of the grant application phase, a formal ethics assessment is carried out by a review panel, resulting in an ethics review report that is made available to the project consortium. The requirements issued by the review panel in turn become contractual responsibilities for the project consortium and, as the Horizon 2020 funding guidelines specify, 'all ethics requirements due after project start are automatically included in the grant agreement in the form of deliverables. These deliverables are known as "ethics deliverables" and will be placed in an automatically generated work package called "ethics requirements".'[6] Through this mechanism, the European Code of Conduct for Research Integrity and the RRI framework become translated into concrete project components. Notably, there is not one pre-specified way in which ethics must be implemented in the design of a research project, and we have witnessed various forms of integration. The following excerpt from the grant agreement for one of our projects illustrates a rather common way in which applied ethics becomes a part of security research:

> All work that is undertaken in the project will be for the benefit of the European citizens. The role of Ethics in the project is significant. Considered as a horizontal work package, it focuses on ensuring that no ethical problems will exist for the final version of the [Project A] framework and through the implementation of the project. The [Project A] consortium is fully aware of the ethical implications of the proposed research and respects the ethical rules and standards of FP7, and those reflected in the Charter of Fundamental Rights of the European Union. [Project A] devotes the whole WP[X] to the investigation of ethical issues and societal impact aspects relevant to the project's field of research, as well as to the monitoring of all technical activities…. Within WP[X], extensive research will result in detailed analysis of ethical and societal issues (T[X].1). The WP[X] Task leader [Institution] is also committed to supervise the project's activity from an ethical and fundamental rights perspective and to provide advice to partners (T[X].2). (Project A Grant Agreement, Part B: 93–94)

As can be seen in the description of applied ethics work in the project, its primary task is here envisioned as 'monitoring' of the technical activities, as well as providing 'advice' to consortium partners. Ethics is in this sense broadly interpreted as 'the world of values that surrounds and flows through any project' (Burgess, 2011a: 3), and the role of the ethics Work Package (WP) corresponds with the manifold normative challenges that can emerge from ongoing research. In practice, such a broad interpretation of ethics and its guidance and advice capacities results in varying forms of ethics work within project consortia, including the likes of establishing a dialogue with technical partners and raising awareness of ethical stakes, input to technical components and processes, provision of best practice guidelines, or the development of evaluation schemes for project components (see, for example, Hempel et al., 2013; Van Gorp

and Van der Molen, 2011). These activities should in theory make it possible to put critique to work and to establish an ethically informed dialogue with those professional communities that are involved in imagining and producing security in the arena of security research programmes. In practice, however, applied ethics are likely to face a considerable number of challenges.

Applied ethics between a rock and a hard place?

The first challenge that we seek to point out is the *organizational structure* of EU-funded research projects. While these are formally supposed to be collaborative and interdisciplinary, in practice the work is divided into WPs that often reproduce disciplinary boundaries and therefore lead to silo structures within a project. Interaction between WPs is at times reduced to handing over results of predefined tasks. As the example of Project A shows, while ethics is within this division of work seen as a cross-cutting issue, it is nevertheless organizationally separated into a dedicated WP. From this separate sphere, ethical advice is supposed to be transferred to the technical parts of the project, the research process supervised, and the product under development evaluated. The ethics WP is in this vein usually presented as running throughout the whole project, as illustrated by diagrams of the project structure that connect the ethics WP to all other WPs by arrows in both directions, thereby signalling to the European Commission that ethics is taken seriously. This looks sound on paper, provided that the project partners are united by a common goal and committed to genuine collaboration to ensure that this goal is achieved.

In the example of Project A, ethics work was structured along three tasks: 'Ethical and Societal Impact Review', 'Ethical Monitoring of the Project's Activities' and the organization of an 'Ethics and Privacy-by-Design Workshop' (Project A Grant Agreement, Workplan Table: 28–29). The role ascribed to ethics is thereby to facilitate a meaningful science–society dialogue by trying to reconcile the conflicting normative orientations of the different exoteric communities involved in the research process – at least that is the theory and the selling point. In practice, however, the separation of ethics from the technical WPs within a project is prone to reinforcing the divide between both problem-solving attitudes in the natural and technical sciences and the pragmatic approaches of practitioners, on the one hand, and the reflexivity that ethics could potentially instil, on the other. This becomes aggravated by the fact that ethics is often grouped together with 'legal' and 'social' issues, thus constituting the ELSI/ELSA category recommended by the Expert Group on Policy Indicators for Responsible Research and Innovation (European Commission, 2015). This results in a combination of diverse questions related to such matters as legal compliance of technical activities and formalized aspects of research governance, such as informed consent agreements or data protection documentation. In practice, these diverse aspects then become outsourced to the ethics WP with the expectation that the 'ethics person' will have the competencies and resources to handle them – a view that is reinforced by the Commission's Guidance Document on the Roles and Functions of Ethics Advisors/Ethics Advisory Boards in EC-Funded Projects (European Commission, 2012d: 3).

In one of our projects, the ethicist was indeed expected to assist the technical partners in identifying relevant national data protection authorities in 10 countries and obtaining documented confirmation from these authorities that the planned research activities would not infringe national data protection legislation, so that these documents could then be presented to the European Commission in order to demonstrate that the project activities were 'ethically approved'. Such a conceptualization of what ethics is and what it can do is, needless to say, a highly reductive one, as it envisions ethics as a way of practically guiding the project through legally and organizationally unclear and messy territory, and has little in common with the idea that ethics should be 'concerned with the definition of the "good" regarding security' (Browning

and McDonald, 2013: 236) or indicate at least partial answers as to the desirability of the direction in which the project is heading and what could or should be done in relation to this. Likewise, it has little in common with the political commitment that ethics should address wider societal implications from research and development activities (see, for example, European Commission, 2013, 2015).

This becomes even clearer when considering the formalized outputs from ethics work within security research projects. Ethics WPs typically produce a set of reports that are separated from the output of the technical WPs. In the example of Project A, these consisted of annual monitoring reports as well as two ethical and societal impact assessment reports (one 'preliminary' version at the halfway stage of the project and one final version at the project's end). Such reports become part of the annual project review conducted by the European Commission, and project leadership needs to formally relate to them. This does not necessarily mean that they will be read and appreciated in their entirety, however. On the contrary, it is our experience that during consortium meetings at which the progress of each WP would be presented, the questions to the ethics WP would usually run along the lines of 'Do you think there is anything unethical, and, if so, what is the action required and who should do it?' Ethics is in this sense treated as a mechanistic practice of addressing yet another set of formal requirements in order not to put the progress of the project at stake – and not as a challenge that provokes debates about the normative desirability of the product under development (or single components of it).

As reflected in the previous point, the second challenge that we seek to highlight is the diversity of *normative orientations* in security research that produce different expectations as to what ethics is and what it is supposed to do. Pertinent here is the prevalent *market dimension* in EU security research that foregrounds efficiency, pro-growth strategies and the economic impact of tools under development (see, for example, European Commission, 2009, 2012b). Closely aligned is the industry perspective on security research that highlights the need for commodifiable solutions, product promotion and market realization (see, for example, Ecorys, 2009; European Commission, 2012a). The role of ethics, from such a perspective, is to ensure societal uptake of the products under development. Ethics is here rendered as a competitive asset in the security business, as it could serve as a label for the acceptability of new technologies and thus contribute to market success (see, for example, Bigo et al., 2014; Hayes, 2006; Jones, 2017).

Such an uncritical understanding of ethics in turn speaks closely to an *alleged neutrality of technology* and a narrative of progress in which technological tools serve to overcome security threats. Through technology-driven change and smart engineering and design – according to the assumption underlying Horizon 2020 – research and development can come up with 'real solutions' for 'real problems'.[7] The social and political complexity of security then becomes reduced to questions of innovative engineering and design, and is made amenable to technological fixes. From such a vantage point, ethics in the sense of critical reflexivity must almost necessarily be perceived as a nuisance that could potentially interfere with straightforward technical rationality. This corresponds with our experiences that ethicists within project consortia are at times confronted with unconcealed hostility, as there is a diffuse fear among the technical partners and end-users that ethics could flag otherwise elegant design and engineering solutions and put them under normative scrutiny. Ethical arguments are in this sense often misinterpreted and perceived within binary categories of 'you can do this'/'you can't do that'. The only half-ironic questions that we were many times confronted with over lunch or coffee whether this or that would be 'ethical' are highly illustrative of this.

Ethics also faces challenges against the backdrop of larger *anticipatory and preemptive trends* in security politics and practices (see, for example, Amoore and De Goede, 2008; Aradau and Van Munster, 2007; Beck, 2002). In our experiences, involved end-users (e.g. police representatives,

civil protection officers, crisis managers) would often 'securitize' the research in question by positing that 'we need to do this, because otherwise we can't catch the bad guys/protect the population/ etc.' and making reference to their professional experience and expertise. In our projects, the professional requirements uttered by end-users would at times brush aside ethical arguments by simply framing them as disruptive and inefficient in terms of solving the specific problem at hand. Ethics from such a perspective then becomes diminished and is depicted as an irrelevant, 'soft' consideration that could only impede the efficient production of security.

These interrelated organizational and normative constraints, reflecting rationales of economy, technology and expertise, are all central problems in security politics and practices highlighted by critical security studies. Taken together, they illustrate aptly how ethics runs the risk of being instrumentalized – that is, how it is presented as an integral part of security research towards the European Commission and the public while being severely restricted in everyday project work. Such instrumentalization tendencies are most vividly demonstrated by the reductionist role that involved exoteric communities ascribe to ethics. A tame and bureaucratic notion of ethics is welcome, as it could indeed ensure the acceptability of the research, support the market uptake of the products under development and contribute to an overall economic strategy that imagines security as a key factor to boost growth. A bothersome and critical form of ethics, however – one that would demand reflexive engagement with one's own positionality and stakes and would problematize the project's goals and contest a presumed technical innocence – is arguably not what most security research projects are looking for, and is thus met with disinclination or even outright rejection. Ironically, this might lead to a conducive market for 'instrumental security ethics', where ethicists would have little interest in critical dialogue but nevertheless justify a project's research activities through their mere participation in the consortium.

Conditions for meaningful critique

Against the backdrop of these challenges that applied ethics is likely to face in the context of security research programmes, with the multiple actors and conflicting rationales at play within concrete projects, the question emerges whether there is room for meaningful critique within such contexts after all. We believe there is. Rather than denying the possibility for critique within the scope of existing political conditions in the first place (and thus calling for radical emancipatory alternatives), we are convinced that constructive dialogue can be conveyed within security research projects. In the best of worlds, applied ethics can in this sense instil reflexivity within involved exoteric communities, serve as a critical corrective early on during research and development activities, and turn hostility into productive engagement. In order to develop this potential, however, we do contend that a number of conditions for meaningful critique must be fulfilled. Therefore, we sketch out several tangible preconditions for successful engagement that must be met in order for the participation of ethics partners within EU security research to be justifiable from a critical security studies perspective.

Our first condition concerns the conflation of ethics with legal questions in ELSI/ELSA categories, as recommended by the Report from the Expert Group on Policy Indicators for Responsible Research and Innovation (European Commission, 2015). This results, as we have shown, in a drawing together of ethics with a wider array of regulatory issues and compliance questions. As the European Commission (2012d: 3) itself points out, ethics should 'cover expertise in law, data protection/privacy and research ethics and substantive experience in the assessment of ethics issues in the specific topic area of the project'. While, from a managerial standpoint, it might be convenient to outsource all conceivable issues that fall outside the actual product development work into a single WP and deal with them in a one-stop-shop fashion, it is unrealistic to expect that all of the

above functions could be fulfilled by ethics. We put forward in this vein that it is necessary to detach ethics from the legal analyses and thereby free it from the role of 'legal compliance watchdog'. Only then can ethics engage involved exoteric communities in reflexive debates on the normative aspects of the production of security.

In close conjunction with the previous point, our second condition concerns the conceptual status of ethics that becomes enabled in EU security research. As we have shown, the reinforced incorporation of ethics into the governance of research activities, while generally mostly perceived as a welcome tendency, ironically brings with it tendencies of overformalization that reduce ethics to a set of predefined categories that fall short of the wealth of relevant theories and conflicting ethical perspectives. What Haggerty (2004) has called 'ethics creep' is epitomized in the apprehension of ethics as a bureaucratic practice where ethics work means going by a checklist and making sure that all of the boxes on the list are ticked. Such a 'fetishization of rules', as he argues, significantly undermines the notion of responsibility and accountability within research itself, and severely constrains ethics work and its capacities (Haggerty, 2004: 410). The European Group on Ethics in Science and Technologies (2014: 71), for instance, identifies a set of analytic and procedural principles (dignity, privacy and freedom, autonomy and responsibility, well-being and flourishing, justice, transparency, efficacy, proportionality) that are relevant within security research, but fails to recognize how these principles are essentially contested and invoke ancient and contemporaneous controversies (see, for example, Cohen and Heath Wellman, 2005; Fitzpatrick, 2008; Singer, 1986).

An ethics that embraces such controversy and is open for contestation and dialogue, such as we put forward here, is however precisely the kind that is needed. In accordance with critical security studies and the commitment to put critique to work, ethics must not be stifled, but rather thrive on dissent and a destabilization of established positions in order to 'reflexively examine the implications of alternative security conceptions and practices in analytical terms' (Browning and McDonald, 2013: 250). It must, moreover, as Fitzpatrick (2008: 5) puts it, '[capture] the abstract, dialogical process of philosophical investigation, while dealing with questions that, although practical, do not lend themselves to quick and easy resolution'. What a critical and reflexive form of ethics can in this sense provide is an analysis of normative challenges in concrete contexts, while at the same time relating them to broader perspectives on society, democracy and justice.

What it can (and should) not provide is a blank cheque form of 'ethical approval' for security products or systems per se. Ethical verdicts, if desirable at all, would depend on contexts of implementation, and moreover rely on contestable political interpretations of normative premises such as human rights or civil liberties. Yet, nonetheless, there is a widespread expectation that the ethics part in security research should determine whether a product is 'ethical' or not in an objective sense, paralleling evaluations of legal compliance. Ethics is in this sense at times perceived as a privileged epistemic perspective that would put an end to all speculation and would inform research as to the right/wrong direction – something that neatly falls in line with the bureaucratized and managerial environment of project management.

Against this backdrop, carving out the necessary space for openness and reflexivity is paramount. Our third condition therefore concerns the forms of input that ethics provides to the work of the project consortium in security research. Such input should not be based on reports alone, but ethics work should involve more creative and interactive methods than the standard format of presentation and ensuing question-and-answer sessions in project meetings. Workshop sessions on ethical aspects of the project's activities (such as the 'Ethics and Privacy-by-Design Workshop' in the example of Project A) where all or select project partners are actively involved offer a more direct and tangible way of raising awareness of possible societal implications of the research and

fostering reflexivity about the role and agency of consortium partners. However, for such sessions to have a genuine impact, they need to be carefully designed and executed. In another project, an internal 'ethics helpdesk' was established, inviting consultations on research design involving ethical stakes. By having these discussions early in the research process, consortium partners had little to lose from being open about their choices and dilemmas.

Succeeding in more interactive forms of ethics work is thereby as much a question of language as it is of interest and attention, and it often includes going into the very basics of applied ethics fields such as computer ethics or media and communication ethics. Computer scientists, engineers and natural scientists are trained in entirely different theoretical landscapes, and expecting them to easily follow ethical reasoning without assistance is not necessarily more realistic than the expectations that ethicists could easily follow technical discussions about how to most efficiently connect the front end of an application with the corresponding database. Productive collaboration across disciplinary boundaries, difficult and exhausting as it may at times be, does however offer great potential with regard to the development of shared ideas and norms, and might accordingly be regarded as key for critical and reflexive thinking (Guillaume, 2015).

Our final condition concerns the political level of oversight. A way to strengthen the influence of ethics and to make sure that it is not reduced to an instrumental function of approval would be that reports are not only distributed internally to the project partners and the European Commission but also to an independent ethics body. This body could review the quality of the reports, ensuring sufficient critical distance and a solid methodology. Moreover, we think that it might even be worthwhile to consider an institution other than the European Commission to execute formal ethical oversight of security research. The Commission has a documented history of seeing security research primarily as an economic tool to boost the European security market and to foster the global competitiveness of the European security industry (see, for example, European Commission, 2009, 2012a, 2012b). Against the backdrop of these vested interests, to instead have ethics WPs report directly to another EU body – such as, for instance, the European Parliament, which has in the past shown far more sensitivity to ethical questions in security research (Bigo et al., 2014; Jeandesboz and Ragazzi, 2010) – would appear a viable strategy. This would grant ethics work an improved standing within project consortia, create incentives for consortium partners to engage in reflexivity, provide valuable feedback to the policymaking world, and not least send out a strong signal to the public that ethics in EU security research will not easily falter amid the multiple cross-pressures to which it is subjected.

Our pragmatic position expressed through these conditions is thereby to provide some form of middle ground between 'deconstructive' forms of critique and 'emancipatory' approaches. We are fully aware at this point of the dangers of instrumentalization and co-option discussed in the previous section – that is, the fact that scholarly engagements can run the risk of sustaining established power structures and institutions rather than critically challenging them (Hynek and Chandler, 2013: 50), as well as of the dangers of overemphasizing normative arguments and thereby losing the analytical focus on the politics and practices of security (Jabri, 2016; Sjoberg, 2013). Nonetheless, we are convinced that critical perspectives on security and a practice-oriented, pragmatic stance can go hand in hand under certain conditions, and we consider applied ethics of this critical kind a viable way of advancing debates about the status of critique by putting it to work in concrete contexts.

This approach in fact speaks closely to already existing forms of engagement from critical security studies and beyond. Scholars, NGOs and reports on behalf of the European Parliament have over the past years called for a stronger role for ethics in European security research and have demanded reinforced attention to the wider societal repercussions of new security technologies (e.g. Bigo et al., 2014; Burgess, 2012, 2014; Hayes, 2006, 2011; Jeandesboz and Ragazzi, 2010;

Jones, 2016). However, as we have shown, stronger formal incorporation of applied ethics in research funding frameworks is not enough. The practical challenges for applied ethics work that we have outlined demonstrate that it is paramount to pay careful attention to the specific ways in which ethics becomes part of security research projects, and what kind of critique becomes enabled or foreclosed amid the multiple stakes and cross-pressures in security research.

Conclusions

As we have argued throughout this article, ethics in EU security research speaks to a number of core concerns in critical security studies: (1) it translates sometimes abstract academic considerations about the status and role of critique into concrete forms of engagement; (2) it serves as a way of getting in touch with the exoteric communities that are involved in imagining and producing security; (3) it creates dialogue between the academic presupposition of reflexivity and the problem-solving attitudes that are prevalent in research and development activities, and thereby implies the need to render critique productive and applicable; (4) it places the normative prescriptions of critical security studies within the political, social, economic and technical contexts of security 'in the making', where it is still subject to debate and technical 'black boxes' have not yet been closed; and (5) it presents a language for relating technical questions not only to regulatory debates on legality but also to political debate on alternative futures. Having concentrated on the concrete challenges that applied ethics work faces vis-a-vis the variegated interests and stakes entrenched in EU security research, we have suggested a number of concrete ways to improve the conditions for meaningful critique. Overall, our argument speaks to wider critical security studies debates on two levels.

First of all, it problematizes practical aspects of critique. The c.a.s.e. manifesto has made the bold claim that 'the goal of a critical intellectual is not only to observe, but also to actively open spaces of discussion and political action, as well as to provide the analytical tools, concepts and categories for possible alternative discourses and practices' (c.a.s.e. collective, 2006: 476). If we accept the premise that critical security scholars should get out of the ivory tower and engage the ways in which security is imagined, engineered and implemented through the work of exoteric communities such as the ones that are involved in security research projects, then we must be prepared to enter into messy real-life practices and be willing to foster dialogues that might be challenging and exhausting. 'Doing critique' in the form of applied ethics requires a substantial amount of work, and even the European Commission (2012d: 11) itself is quite straightforward about the fact that 'there is no doubt that serving as an Ethics Advisor on a major project is a very challenging and demanding job and requires a great deal of dedication, experience, commitment and enthusiasm'.

Putting critique to work in this sense means to engage in translation exercises between different disciplines, stakes, rationales and argumentative cultures – all while struggling to maintain an open space for debate and contestation and resisting the dangers of instrumentalization and co-option. Furthermore, debates within critical security studies and ethics as to what 'good' security could look like further complicate the stakes of such an endeavour. But ultimately, so we put forward here, these issues are part of the deal for an academic field that deems itself 'critical'. Claims about what should be done, who should be engaged and how, and which research objects should be on the agenda are quickly made, but hard to follow through with rigor and resolution.

The case of EU security research shows how easily critique can falter, be overheard or be co-opted against the backdrop of the powerful cross-pressures of markets, politics, end-users and an overall narrative of technical progress. Accordingly, it resonates with ongoing debates about the suitability of scholarly critique for generating political change and its potential to do so in the first

place (e.g. Boltanski, 2011; Bourdieu, 2000; Hutchings, 2001; Latour, 2004). In this sense, a pertinent question for critical security studies is the one concerning the fragile balance between the justifiability of and the responsibility for 'getting one's hands dirty' – be it by offering emancipatory alternatives, entering processes of policymaking or engaging the complex world of security research where one has to navigate between different normative orientations, reconcile largely incompatible disciplinary languages, resist strong sectorial pressures and attempt to enact critique by fostering reflexivity in a reflexivity-averse environment.

In the words of Flyvbjerg (2001: 139), the goal of a critical stance must be 'to produce input to the ongoing social dialogue and praxis in a society, rather than to generate ultimate, unequivocally verified knowledge'. This is, as he argues, the unique strength of the social sciences, and we put forward here that critical security scholars should not refrain from this task as long as conditions for meaningful critique are given. Entering the security research arena through applied ethics presents us with a tangible way of engaging exoteric communities that are otherwise sometimes hard to get in touch with, and security research will remain high on the agenda of the EU (and other countries) for the foreseeable future. Even if results from funded projects do not always end up being implemented (Biermann and Fuchs, 2017; Tokmetzis and Goslinga, 2017), there is intrinsic value in such critical engagement – and individuals and institutions that take part in EU security research are also involved in many other security-related activities, meaning that they can in the best case serve as multipliers for more critical and reflexive attitudes towards security and its production.

The second problematization that we see with regard to critical security studies is a necessary conceptual clarification concerning the notion of ethics. While ethics serves as a regular point of reference in literature that engages the normativity of security, it remains at times unclear what kind of 'ethics' is precisely referred to. In our view, there is thus a need not only to reconsider the role of critique within the field, but also at the same time to reflect what kind of ethics critique presupposes. Ethics, as we have argued, can serve as a tangible and politically recognized way of engaging practical ways of imagining and producing security. There is, however, a risk that ethics becomes reduced to a formalized and blunted instrument that serves the intertwined interests of politics, markets and practitioners. Instead, we propose that ethics should play to its strengths as a mode of reflexivity that challenges normative assumptions vis-a-vis actor positionality and wider trajectories of democracy and justice.

Ethics, so we put forward here in line with both theoretical considerations and personal experience, cannot unequivocally determine what 'good' security is. Under the right conditions, however, it can scrutinize the normative implications of security in specific environments – for example, in technical or organizational contexts. Ethics should thereby challenge and problematize presupposed security problems and security solutions, and encourage reflexivity among the involved stakeholders. Notably, it should at the same time favour constructive and practically oriented ways of convening critique. If critical security scholars need to clearly position themselves vis-a-vis the status and meaning of critique, as this special issue suggests, then they should also engage in debates about the nature and status of ethics. While there are important ventures into this direction (e.g. Bigo, 2002; Browning and McDonald, 2013; c.a.s.e. collective, 2006; Der Derian, 1995; Huysmans, 1998), the issue of ethics with regard to a critical understanding of studying security remains an underexplored one. Critique and ethics are certainly not the same thing, but critical security studies is to a large extent premised on ideas of a more just and inclusive society, thereby creating a sizeable overlap with ethical analyses. From our analysis of the example of ethics in EU security research, we may conclude that the combination of the two can be particularly fruitful, as a critical analysis of power serves to clarify the conditions under which ethical engagement may succeed.

Acknowledgements

Funding

Notes

1. See http://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/applying-for-funding/find-a-call/h2020-structure-and-budget_en.htm (accessed 15 July 2018).
2. See https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens (accessed 15 July 2018).
3. See http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm (accessed 15 July 2018).
4. See http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm (accessed 15 July 2018).
5. 'ELSI/ELSA' is the common abbreviation for 'ethical, legal and social/societal issues/aspects'.
6. See http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm (accessed 15 July 2018).
7. EU Commissioner for Research, Science and Innovation Carlos Moedas in a speech on 'The Future of Market-Creating Research and Innovation in Europe' at the Centre for European Economic Research, Mannheim, 13 April 2016; see https://ec.europa.eu/commission/commissioners/2014-2019/moedas/announcements/future-market-creating-research-and-innovation-europe_en (accessed 15 July 2018).

References

ALLEA (2017) *The European Code of Conduct for Research Integrity*, rev. edn. Berlin: ALLEA – ALL European Academies.

Amoore L and De Goede M (eds) (2008) *Risk and the War on Terror*. London & New York: Routledge.

Aradau C and Van Munster R (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13(1): 89–115.

Beck U (2002) The terrorist threat: World risk society revisited. *Theory, Culture & Society* 19(4): 39–55.

Biermann K and Fuchs C (2017) 800,000 euros for a terror air bag that never got made. *Die Zeit*, 23 February. Available at: http://www.zeit.de/wirtschaft/2017-02/security-technologies-eu-terror-research-fraunhofer/komplettansicht (accessed 15 July 2018).

Bigo D (2002) Security and immigration: Toward a critique of the governmentality of unease. *Alternatives: Global, Local, Political* 27(1): 63–92.

Bigo D, Jeandesboz J, Martin-Mazé M and Ragazzi F (2014) Review of security measures in the 7th Research Framework Programme FP7 2007–2013. Brussels: European Parliament.

Boltanski L (2011) *On Critique: A Sociology of Emancipation*. Cambridge: Polity.

Booth K (1991) Security and emancipation. *Review of International Studies* 17(4): 313–326.

Booth K (ed.) (2005) *Critical Security Studies and World Politics*. Boulder, CO & London: Lynne Rienner.

Bourdieu P (2000) *Pascalian Meditations*. Stanford, CA: Stanford University Press.

Browning CS and McDonald M (2013) The future of critical security studies: Ethics and the politics of security. *European Journal of International Relations* 19(2): 235–255.

Burgess JP (2011a) Ethical review and the value(s) of security research. Paper presented at the workshop on Ethical Issues in Security Research: A Practical Approach, Brussels, 29 September.

Burgess JP (2011b) *The Ethical Subject of Security: Geopolitical Reason and the Threat Against Europe*. Milton Park & New York: Routledge.

Burgess JP (2012) The societal impact of security research. PRIO Policy Brief 09/2012. Oslo: PRIO.

Burgess JP (2014) The future of security research in the social sciences and humanities. Strasbourg: European Science Foundation.

Burke A (2013) Security cosmopolitanism. *Critical Studies on Security* 1(1): 13–28.

c.a.s.e. collective (2006) Critical approaches to security in Europe: A networked manifesto. *Security Dialogue* 37(4): 443–487.

Cohen AI and Heath Wellman C (eds) (2005) *Contemporary Debates in Applied Ethics*. Malden, MA: Blackwell.

De Goede M (2011) European security culture: Preemption and precaution in European security. Inaugural lecture, University of Amsterdam, 27 May 2011.

Der Derian J (1995) The value of security: Hobbes, Marx, Nietzsche, and Baudrillard. In: Lipschutz RD (ed.) *On Security*. New York & Chichester: Columbia University Press, 24–45.

Ecorys (2009) *Study on the Competitiveness of the EU Security Industry: Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054. Final Report*. Brussels: Ecorys Research and Consulting.

European Commission (2009) A European Security Research and Innovation Agenda: Commission's initial position on ESRIF's key findings and recommendations. COM(2009)691 final. Brussels, 21 December.

European Commission (2012a) Action plan for an innovative and competitive security industry. COM(2012)417 final. Brussels, 26 July.

European Commission (2012b) EU security research: Safeguarding society, boosting growth. Luxembourg: Publications Office of the European Union.

European Commission (2012c) Responsible research and innovation: Europe's ability to respond to societal challenges. Brussels.

European Commission (2012d) Roles and functions of ethics advisors/ethics advisory boards in EC-funded projects. Brussels.

European Commission (2013) Options for strengthening Responsible Research and Innovation: Report of the Expert Group on the State of Art in Europe on Responsible Research and Innovation. Brussels.

European Commission (2015) Indicators for promoting and monitoring Responsible Research and Innovation: Report from the Expert Group on Policy Indicators for Responsible Research and Innovation. Brussels.

European Commission (2016) H2020 programme guidance: How to complete your ethics self-assessment. Version 5.2. Brussels.

European Commission (2017a) H2020 programme: Multi-beneficiary general model grant agreement (H2020 General MGA – Multi). Brussels.

European Commission (2017b) Responsible Research & Innovation. HORIZON 2020: The EU Framework Programme for Research and Innovation. Available at: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation (accessed 2 October 2018).

European Group on Ethics in Science and New Technologies to the European Commission (2014) Ethics of security and surveillance technologies. Luxembourg: Publications Office of the European Union.

European Union (2000) Charter of fundamental rights of the European Union. 2000/C 364/01. 18 December.

Fierke KM (2007) *Critical Approaches to International Security*. Oxford: Polity.

Fitzpatrick T (2008) *Applied Ethics and Social Problems: Moral Questions of Birth, Society and Death*. Bristol: Policy Press.

Flyvbjerg B (2001) *Making Social Science Matter: Why Social Inquiry Fails and How It Can Succeed Again*. Cambridge: Cambridge University Press.

Garber M, Hanssen B and Walkowitz RL (2000) Introduction: The turn to ethics. In: Garber M, Hanssen B and Walkowitz RL (eds) *The Turn to Ethics*. New York & London: Routledge, vii–xii.

Grunwald A (2014) The hermeneutic side of responsible research and innovation. *Journal of Responsible Innovation* 1(3): 274–291.

Guillaume X (2015) Collaboration. In: Aradau C, Huysmans J, Neal AW and Voelkner N (eds) *Critical Security Methods: New Frameworks for Analysis*. Milton Park & New York: Routledge, 189–207.

Haggerty KD (2004) Ethics creep: Governing social science research in the name of ethics. *Qualitative Sociology* 27(4): 391–414.

Hayes B (2006) *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: Transnational Institute/Statewatch.

Hayes B (2011) Rethinking the EU Security Research Programme. Submission by Statewatch in response to Section 4 ('Securing the Citizen and the Society') of the European Commission's Consultation on an Industrial Policy for the Security Industry. Available at: http://www.statewatch.org/analyses/no-133-esrp-consultation-response.pdf (accessed 15 July 2018).

Hempel L, Ostermeier L, Schaaf T and Vedder D (2013) Towards a social impact assessment of security technologies: A bottom-up approach. *Science and Public Policy* 40(6): 740–754.

Hoijtink M (2014) Capitalizing on emergency: The 'new' civil security market in Europe. *Security Dialogue* 45(5): 458–475.

Hutchings K (2001) The nature of critique in critical international relations theory. In: Wyn Jones R (ed.) *Critical Theory & World Politics*. Boulder, CO & London: Lynne Rienner, 79–90.

Huysmans J (1998) Security! What do you mean? From concept to thick signifier. *European Journal of International Relations* 4(2): 226–255.

Hynek N and Chandler D (2013) No emancipatory alternative, no critical security studies. *Critical Studies on Security* 1(1): 46–63.

Jabri V (2016) Security: Critique, analysis and ethics. In: Nyman J and Burke A (eds) *Ethical Security Studies: A New Research Agenda*. Milton Park & New York: Routledge, 17–31.

Jeandesboz J and Ragazzi F (2010) Review of security measures in the Research Framework Programme. Brussels: European Parliament.

Jones C (2016) The visible hand: The European Union's security industrial policy. Statewatch Analysis no. 19/16, August 2016. Available at: www.statewatch.org/analyses/no-297-security-industrial-policy.pdf (accessed 15 July 2018).

Jones C (2017) Market forces: The development of the EU security–industrial complex. Amsterdam/London: Transnational Institute/Statewatch.

Krause K and Williams MC (eds) (1997) *Critical Security Studies: Concepts and Cases*. London: Routledge.

Latour B (2004) Why has critique run out of steam? From matters of fact to matters of concern. *Critical Inquiry* 30(2): 225–248.

Leese M (2017) Holding the project accountable: Research governance, ethics, and democracy. *Science and Engineering Ethics* 23(6): 1597–1616.

Nunes J (2012) Reclaiming the political: Emancipation and critique in security studies. *Security Dialogue* 43(4): 345–361.

Nyman J and Burke A (eds) (2016a) *Ethical Security Studies: A New Research Agenda*. Milton Park & New York: Routledge.

Nyman J and Burke A (2016b) Introduction: Imagining ethical security studies. In: Nyman J and Burke A (eds) *Ethical Security Studies: A New Research Agenda*. Milton Park & New York: Routledge, 1–14.

Official Journal of the European Communities (1998) Decision No 182/1999/EC of the European Parliament and of the Council of 22 December 1998 concerning the Fifth Framework Programme of the European Community for Research, Technological Development and Demonstration Activities (1998 to 2002). Brussels.

Official Journal of the European Union (2007) Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (2007/C 306/01). Brussels.

Official Journal of the European Union (2013) Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in 'Horizon 2020: The Framework Programme for Research and Innovation (2014–2020)' and repealing Regulation (EC) No 1906/2006. Brussels.

Owen R, Macnaghten P and Stilgoe J (2012) Responsible research and innovation: From science in society to science for society, with society. *Science and Public Policy* 39(6): 751–760.

Owen R, Bessant J and Heintz M (eds) (2013) *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Chichester: Wiley.

Protection and Security Advisory Group (2016) Horizon 2020 – Societal Challenge 7: Secure societies – Protecting freedom and security of Europe and its citizens. Report of the Protection and Security Advisory Group. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/poli-cies/security/report_of_the_h2020_protection_and_security_advisory_group_-_pasag_en.pdf (accessed 15 July 2018).

Singer P (ed.) (1986) *Applied Ethics*. Oxford: Oxford University Press.

Sjoberg L (2013) The paradox of security cosmopolitanism? *Critical Studies on Security* 1(1): 29–34.

Tokmetzis D and Goslinga M (2017) How billions vanish into the black hole that is the security industry. *De Correspondent*, 22 February. Available at: https://thecorrespondent.com/6229/how-billions-vanish-into-the-black-hole-that-is-the-security-industry (accessed 15 July 2018).

Valkenburg G (2017) Security technologies versus citizen roles? *Science as Culture* 26(3): 307–329.

Van Gorp A and Van der Molen S (2011) Parallel, embedded or just part of the team: Ethicists cooperating within a European security research project. *Science and Engineering Ethics* 17(1): 31–43.

Von Schomberg R (2011) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields: A Report from the European Commission Services*. Brussels: European Commission.

Williams MC and Krause K (1997) Preface: Toward critical security studies. In: Krause K and Williams MC (eds) *Critical Security Studies: Concepts and Cases*. London: Routledge, vii–xxii.

Matthias Leese is a Senior Researcher at the Center for Security Studies, ETH Zurich, Switzerland.

Kristoffer Lidén is a Senior Researcher and Research Director at the Peace Research Institute Oslo (PRIO), Norway.

Blagovesta Nikolova is a Post-Doctoral Researcher at the Bulgarian Academy of Sciences, Sofia.