Forthcoming in

Calcara, Antonio, Raluca Csernatoni, Chantal Lavallée eds (2020) *Emerging Security Technologies and EU Governance Actors, Practices and Processes*, Routledge.

The security politics of innovation: Dual-use technology in the EU's security research programme

Bruno Oliveira Martins (Peace Research Institute Oslo)

Neven Ahmad (University of Oslo)

Abstract

This chapter addresses the central role played by dual-use technologies in security and defence research policies of the European Union. It puts forward the argument that the EU's strong incentives to these technologies – on the grounds of its potential for generating economic, industrial and innovation synergies between the civilian and the military domains – are a political choice that has relevant consequences in the security politics of the Union. The chapter provides an overview of the main academic debates surrounding the concept of dual-use technologies in different academic fields and it contributes to these discussions through a Science and Technology Studies–inspired analysis of the EU reality. Our contribution argues for the necessity of further dialogue between intellectual traditions emanating from STS and critical approaches to security and military studies.

Introduction

In 2007, the European Union (EU) initiated the Framework Programme 7 (FP7), the Union's Research and Innovation funding programme for the period 2007-2013. Totalling over € 50 billion, FP7's budget marked a substantial increase compared with the previous Framework Programme FP6 (41% at 2004 prices), a "reflection of the high priority of research in Europe" (European Commission 2007). With a budget representing two thirds of the overall budget, the core of FP7 was the Cooperation programme that was divided in ten themes, one of which was "Security"[1]. This was the first time that security research had a dedicated theme in the EU's framework programme for research and innovation, and the following programme, Horizon 2020, continued along these lines, having "Secure Societies" as a programmatic area. This security research funded through the EU's framework programmes constitutes the security research programme (SRP). Security-related research in FP7 was "expected to generate new knowledge and promote the application of new technologies in the field of civil security" and would "reinforce the competitiveness of the European security industry by stimulating the cooperation of providers and users for civil security solutions" (ibidem).

Due to its civilian nature, the SRP prevented direct funding of defence and military technology. Yet, it enabled funding for dual-use technology, i.e. technology that can have both civilian and military application. Since then, the provision qualifying dual-use technology as eligible for receiving EU R&D funding has been instrumental for the development of new security technologies in Europe and for a number of different actors, including defence companies, to partake in EU-funded consortia that aim at developing 'security solutions' employing this type of technology (see Introduction in this book).

Like in other developed economies, the EU has equated increased security in the civilian realm with cutting-edge technology. As we will show in this chapter, the SRP pursued

---

1 The other nine themes were Health; Food, agriculture and fisheries, and biotechnology; Information and communication technologies; Nanosciences, nanotechnologies, materials and new production technologies; Energy; Environment (including climate change); Transport (including aeronautics); Socio-economic sciences and the humanities; and Space.

technology-based solutions for security problems. Yet the processes by which civilian technologies get military use (spin-in processes) are becoming increasingly common due to a combination of factors such as declining military expenditure, a highly innovative civilian industry, and a more capability-oriented approach to military innovation (Verbruggen 2019: 338-339). For this reason, a strict distinction between civilian and military technology has become increasingly difficult to draw, and in this context the concept of dual-use technology requires further scrutiny, particularly when it is explicitly promoted by political authorities.

While the SRP has received some attention from different theoretical perspectives, including critical security studies and sociology of knowledge production (Jeandesboz and Ragazzi 2010; Bigo et al. 2014; Edler and James 2015; Lavallée 2016; Carmel 2017, Leese et al 2019, Martins and Küsters 2019), the centrality of the concept of dual-use technology in the broader picture of EU's security and defence research policies demands further inquiry and a multidisciplinary view that can illuminate both the sociological aspects of dual-use technology and the security politics associated with it (see also Molas-Gallart 2002). The process by which the EU has promoted dual-use technology brings new elements for assessing civil-military relations within the EU, sheds light on how the politics of security meets the politics of innovation, and how the notion of dual-use technology has acted as a legitimizing strategy facilitating current spending on defence research (see Calcara and Fiott in this book).

The chapter offers a critical de-construction of these developments through theoretical debates around the concept of dual-use technology in the disciplinary fields of innovation studies and Science and Technology Studies (STS). In its final section, the chapter promotes 'technology' as a conceptual arena where a dialogue between STS and critical approaches to security and militarism should take place.

Dual-use technology: controversies in the literature

At face value, the notion of dual-use technology as one that can have both civilian and military applications is very simple. Yet, any further consideration associated with this basic idea –how is the technology transferred from one field to the other, who defines

what counts as a military application, what regulatory challenges do technology transfers imply, how to know something is potentially benign or malign, etc – has been subject to much inquiry in different academic fields.

The concept of dual-use entered the discourse on weapons and technology exports following World War II (Reppy 1999). This was unsurprising, considering that nuclear technology had the immense destructive power demonstrated in Hiroshima and Nagasaki in 1945, but also offered the promise of a new source of energy; in this case, uranium enrichment plants may produce nuclear fuel for nuclear power plants, but also highly enriched uranium for a nuclear bomb. In the highly politicized and securitized Cold War environment, debates around dual-use technology were an important part of the strategic and geopolitical considerations of the time.

In the Cold War period, dual-use was framed mostly from an arms control perspective. The possibility of using a particular technology for both civilian and military purposes created a problem for the control and diffusion of cutting-edge weaponry (Brauch et al. 1992), in particular as advances in different scientific fields such as biotechnology, neurosciences and genetics created new possibilities for the conduct of war and the resort to political violence. In essence, this quarrel between the promise of scientific progress and the potential threat of a violent destruction constitutes what in the literature has been labelled the dual-use dilemma.

The public and political perception of dual-use technology has changed over time, following wider societal trends about the promise of scientific evolutions for the resolution of different problems. In many ways, then, dual-use technology became gradually perceived also as industrial issue, in the way that it constitutes as an opportunity to provide a wider exploitation of research and manufacturing beyond a given technology's initial objectives, whether they were military or civilian (Molas-Gallart 1997). Along with the perception of the technology, the dual-use dilemma in the security realm has also began to shift, from a narrative about the concern of the dual utility of research in military and civilian settings towards dual-use conversations which focus on how security enterprises should know when (and when not) to classify research, objects, or even people as security threats (Vogel et al. 2017).

Te Kulve and Smit (2003) use the work of Gummett (1991) to show that the distinction between military and civilian technology can be understood as being institutional, rather than intrinsic. Te Kulve and Smit (2003) illustrate that rather than an intrinsic feature of the technology itself, the civilian, military, or dual-use character of a technology is often the result of its shaping within socio-technical networks; that is, not only the shaping of the technology but also the dual-use meaning attached to it depend on its institutional and cultural context. In the article, Te Kulve and Smit show how the bipolar lead-acid battery emerged in a military context in The Netherlands, where the Royal Netherlands Navy envisaged using the battery on future warships; at this initial stage, no civilian application was foreseen. Due a number of circumstances explored in the article, the research institute TNO, in particular its Environment, Energy and Process innovation laboratory (TNO-EEP), became involved in the project, and it was the fact that the TNO-EEP is a "dual oriented institute" that allowed the battery to be understood as having potential civilian application (Te Kulve and Smit 2003: 961-962).

Therefore, dual-use is a dynamic and shifting concept, meaning that the civil, military, or dual-use understandings attached to a technology may change, for example, during the development of the technology in interaction with changes in the number and nature of the actors involved in its socio-technical network (Te Kulve and Smit 2003)[2]. The concept of dual-use technology, then, stands at the crossroads between two opposing views of technology: one that understands technology as artifacts and products *versus* technology as comprising of a whole system of social relations (Molas-Gallart 1997).

A potentially dual-use technology may never be operationalized in all its capacities, and by the same logic, its duality can disappear, or it can appear late in its development and evolution based on the social network of the technology. Cowan and Foray (1995) explore the patterns of potential duality in order to establish the organizational and informational conditions that are required to realize the duality potential. They make a distinction between 'spillover' and duality based on the premise that duality is not intrinsic but rather dependent on the networks that the technology is designed and used in. 'Spillover' is defined as a situation in which the research is conducted within one

2 Still, Haico te Kulve and Wim A. Smit (2003) argue that given a certain social-cultural setting, certain technologies will be more suitable for applications in both domains than others.

domain and then adopted without change to another domain. Therefore, spillovers are not evidence of duality, but rather evidence of its absence, and so the promotion of spillover can be viewed as a policy designed to correct the 'duality failure' of an R&D programme (Cowan and Foray 1995). Molas-Gallart (1997) defines dual-use technology transfer as "a special instance of technology transfer across applications that takes place when a dual-use technology developed for a military (or civilian) use, is transferred to a civilian (or military) application". Therefore, dual-use technology is directly connected to dual-use technology transfers which refers to the case when there is an intention to change the initial (military or civilian) application of a technology.

Alic et al. (1992) interpret military and commercial technological innovation as two systems that draw on a common technical knowledge but that involve two distinct institutions that operate differently. While the commercial industry depends on improving products through a feedback loop with clients, the military industry works with a different logic (see introduction in this book and Alic 1994). The differences extend to goals, technical requirements and managerial arrangements, as a result in most cases military and commercial innovations have evolved distinctive technical 'cultures' (Alic 1992: 43).

The existence of a debate around everything that relates with the concept dual-use technology has important consequences. In the formulation of Molas-Gallart (1997: 370),

> (g)iven its imprecision, it can easily fall prey to political orchestration. It can be used for instance, as a new, more palatable way of presenting measures of support to an industry that has lost some of its capacity to draw political backing.

In the next sections, we will show how this idea is fundamental for understanding the role played by the concept of dual-use technology in the development of the EU's security research programme.

Critical security and military studies approaches

The debates in the fields of innovation studies and STS, briefly introduced above, open relevant opportunities for intellectual cross-fertilization with critical approaches to security and military studies. Even though the field for interdisciplinary exchange remains scarcely explored, some relevant incursions on this dialogue have been observed. These have focused on two main inter-related issues: circulation and ethicalization.

Literature on critical security studies has pointed out how security concerns have converged with ethical dilemmas related to the governing of science. For critical security studies with a Foucaultian inspiration, dual-use emerges as a problem of organizing circulations. For Foucault, circulation is "the space of the operations of human beings and defines the principle of organization of modern biopolitics" (Ceyhan 2012). As explained by Aradau and Blanke (2010: 44), security to Foucault referred to biopolitical practices of 'organising circulation, eliminating its dangers, making a division between good and bad circulation, and maximizing the good circulation by eliminating the bad' (Foucault 2007: 18). From this perspective, policing scientific knowledge through the establishment of a 'culture of responsibility' can be understood as a part of broader shifts towards the subjectification of knowledge (Rychnovská 2016). For Foucault, then circulation is in fact at the heart of modern security governance, constituting freedom and security as two complementary parts of the same system. Rychnovská argues that security concerns have converged with ethical dilemmas related to the governing of science causing an 'ethicalization' of security. From this perspective, then, this 'ethicalization' impacts the politicization of security expertise (Berling and Bueger 2015), prospects of resistance and the democratic accountability of science. Ethicalization leads to moving an issue from the sphere of democratic deliberation not due to the immediate threat but rather on the need to uphold ethical norms (Rychnovská, 2016).

The place of ethics in security research in a European context has been further explored by Leese, Lidén and Nikolova (Leese et al 2019). In their analysis of the place and function of ethics in the EU security research field – a field marked by the centrality of dual-use technology – they note how applied ethics faces challenges resulting from its 'location in the middle of numerous cross-pressures, such as political ambitions, economic interests, technological rationales and the demands of security professionals', which in turn "risk turning what was intended to be the critical corrective of applied

ethics into a legitimizing function of mere 'ethics approval"' (Leese et al 2019: 59). Indeed, these reflections bring new elements for a critique of the dual-use dilemma and expand the contours of its debate. In particular, they relate to a broader discussion on the regulation of scientific and technological developments (see also Burgess et al 2018; Hurlbut 2015). To prevent the conversion of life sciences into 'death sciences' (Atlas and Dando 2006: 277), the United States established a new category of research that is subject to specific regulation. This 'dual-use research of concern' is defined as

> life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security. (US Government, 2014b: 3)

As mentioned above, the regulation of emerging dual-use technologies and their control has been a classic theme in military studies. Yet, recent critical military studies approach open new opportunities for exploring the phenomenon. When addressing the question of what is critical military studies (CMS), Basham, Belkin and Gifkins address three main arenas of inquiry: the triangle practices/institutions, social practices and political contestation; CMS and the exploration of the 'in-between'; and interdisciplinarity and the place of technology in military discussions (Basham et al 2015). These areas invite an interpretation of dual-use technology as an arena to re-question civil-military relations as well as a critical understanding of military socio-technical networks and the governance of weapons innovation. For CMS, then, STS, with its focus on the sociological elements of the process of technology production, can impact military studies by providing a crucial critical conceptual deconstruction and re-equation of military equipment and the political sociological elements that surround it.

An STS-inspired framework

The literature debates introduced above lay the ground for this chapter's theoretical framework, through which the EU's engagement with, and promotion of, dual-use technology will beintroduced. Even though we do not have the space to provide a deep analysis of the topic, we propose this theoretical framework to conduct further studies of different, sectorial analysis of the governance of dual-use technologies in the EU. We draw insights from different bodies of literature that have had relevant contributions to academic debates on the topic, but we put an emphasis on the STS-based inquires. There are two main reasons driving our option. Firstly, the aspects surrounding socio-political aspects of technology development and innovation are the ones that have made the most relevant contributions to the dual-use question (Molas-Gallart 1997, Vogel et al 2017) and therefore they are the ones that can help us drive forward an informed discussion on the European governance of these technologies. Secondly, because many STS-based approaches share epistemological assumptions with critical approaches to security and military studies, this creates a favourable ground for theoretical innovation and contributes for a necessary cross-fertilisation between these areas of knowledge.

From these different bodies of literature, and in particular inspired by Vogel et al (2017), we build a framework of analysis around four ideas: developments in the dual-use dilemma; upstream and participatory governance of security concerns; the politics of security knowledge; and Responsible Research and Innovation.

a) Developments in the dual-use dilemma

Dual-use dilemma arises when a research finding or technology has the potential to be used for both civilian purposes and to be weaponized. This debate is by its nature an ethical dilemma (Selgelid, 2009) and it is mobilized around all forms of dual-use technology, perhaps particularly in the field of biotechnology where for example the positive potential of genetic engineering can lead to a dangerous virus that could have the potential to kill millions (see also Pustovit and Williams 2008; Rath et al 2014). Discussions on this topic shed light on important concepts regarding responsibility, and question what is the responsibility of scientists in fully understanding the possible negative impact of their research findings.

Yet the character of the dual-use dilemma has begun to shift. For Vogel et al (2017:977)

> Where once the primary concern was for the dual utility of research in military and civilian settings, today dual-use conversations focus instead on how security enterprises should know when (and when not) to classify research, objects, or even people as security threats.

today discussion around dual-use technology emphasize the potential industrial benefits of these technologies, and look less into the security aspects that traditionally used be mostly associated with it.

b) Upstream and participatory governance of security concerns

Related with the dual-use dilemma are the idea of expertise and regulation. In other words, navigating the dilemma requires expertise to identify the full spectrum of possibilities emanating from the technology, in particular the full scope of potential threats associated with it. Due to this knowledge requirement, scientists and technology developers are often interested in contributing to the regulation of a particular scientific and technological field, with an understanding that governmental regulation stifles important research while possibly violating academic freedom and in some cases freedom of speech (Selgelid 2009). Associated with the dual-use dilemma is then the broader issue of the regulation of knowledge and scientific developments, as well as the relations between scientists and tech developers with the governance of the future. Upstreaming then is the idea that "broader public input involving a diverse array of expertise is needed on these contentious issues in order to have a more holistic understanding of the issues, problems, stakeholders, values, and agendas at play" (Vogel et al 2017: 978; see also Resnik 2010; and Rychnovská 2016 on how the need for a 'bottom-up' approach with members of the specific fields is required for the creation of codes of conduct).

c) The politics of security knowledge

In the field of dual-use technology, the crucial issue at stake involving the politics of knowledge is how we know something is benign or malign as well as what it *is* in the first

place (Vogel et al. 2017: 979; Hecht 2010). The politics of knowledge examines the interworking of who creates knowledge and for what purpose. In our case, it asks the question: who has the capacity to identify knowledge or a technology as a security issue? This question naturally opens up a larger set of questions that are at the core of critical security studies research agenda, namely: what counts as a security issue? Security for whom, and security from what?

d) Responsible Research and Innovation

Responsible Research and Innovation (RRI) has gained a central position in the EU science and research policies. RRI emerges from the recognition of the power of science, and this recognition has forced reconsiderations of the responsibilities that should follow such power (Stilgoe and Guston 2017; Burgess 2018). Owens et al. (2012) argue that there are three main discourses associated with the idea of RRI: an emphasis on the democratic governance of the purposes of research; the idea of responsiveness (emphasizing established approaches of anticipation in research and innovation); and the framing of responsibility itself in the context of research and innovation as collective activities with uncertain and unpredictable consequences (Owens et al. 2012). Yet, as will be explored below, recent research on the SRP (Martins and Küsters 2019; Leese et al 2019) has showed that the logic of the RRI approach seems to be challenged in important ways by the prominence of the security consortia created through the SRP.

Dual-use technology in EU security and defence research

The Security Research Programme

From the outset, the security research funded under the FP7 had a very strong technological component. The areas to be covered by the SRP, illustrated in Table 1, included technology solutions for civil protection, bio-security, protection against crime and terrorism; border security technologies; technologies for communications, security systems integration, interconnectivity and interoperability. With a total budget of € 1400 million, the SRP had the expectation of both generating new knowledge and promoting

the application of new technologies while reinforcing the competitiveness of the European security industry. In this logic, we can observe the way in which the EU has seen improved security, advanced technology, and industrial development as fully integrated.

Table 1 – Areas for security research under FP7 (Source: European Commission 2014)

Area	Description
Security of citizens	technology solutions for civil protection, bio-security, protection against crime and terrorism
Security of infrastructures and utilities	examining and securing infrastructures in areas such as ICT, transport, energy and services in the financial and administrative domain
Intelligent surveillance and border security	technologies, equipment, tools and methods for protecting Europe's border controls such as land and coastal borders
Restoring security and safety in case of crisis	technologies and communication, co-ordination in support for civil, humanitarian and rescue tasks
Security systems integration, interconnectivity and interoperability	information gathering for civil security, protection of confidentiality and traceability of transactions
Security and society	acceptance of security solutions, socio-economic, political and cultural aspects of security, ethics and values, social environment and perceptions of security
Security research co-ordination and structuring	co-ordination between European and international security research efforts in the areas of civil, security and defence research

The triangle security-technology-industry was further promoted in Horizon 2020, the framework programme that followed FP7. Its security programme was called *Secure Societies* and it comprised the areas displayed in Table 2.

Table 2 – Areas for security research under Horizon 2020 Secure Societies (Source: European Commission 2019)

Area	Description

Natural and man-made disasters	Enhance the resilience of our society against natural and man-made disasters, ranging from the development of new crisis management tools to communication interoperability, and to develop novel solutions for the protection of critical infrastructure
Crime and terrorism	Fight crime and terrorism ranging from new forensic tools to protection against explosives
Border security	Improve border security, ranging from improved maritime border protection to supply chain security and to support the Union's external security policies including through conflict prevention and peace building
Cyber-security	Provide enhanced cyber-security, ranging from secure information sharing to new assurance models.

Besides the SRP areas enunciated above, the EU has established numerous opportunities for the design and implementation of dual-use in the 2014-2020 programming period. Taken together, the European Structural and Investment Funds (ESIF), Horizon 2020, COSME and Erasmus+ programmes provide specific support for the various levels of development within the dual use field. ESIF supports technology transfer, market intelligence, proof of concept and more, and these steps help businesses diversify or move from one sector to another. Horizon 2020 provides funding opportunities to civil application of projects with dual-use nature, while the COSME programme presents opportunities to access certain funding for cooperation between clusters and for partnership-building. Finally, a strand of Erasmus+ contributes to the dual-use expansion by helping to create industry-university collaboration in this field. Through these programmes, all EU companies can benefit from the support of R&D through ESIF and Horizon 2020. Additionally, SMEs are able to benefit from COSME, Horizon 2020 and ESIF (European Commission 2014b).

From security to defence research

The EU views dual-use technology as a way forward for advancing innovation in Europe and the EU's strategic autonomy in the field of security and defence. Importantly, as explored in Martins and Küsters (2019), dual-use research within the SRP created

practices, procedures and cultures that facilitated the opening up to EU-funded defence research operated since 2016 (see also James 2018 on the differences between the SRP and the defence research programme). Jean-Claude Juncker, former president of the European Commission, has made it clear that, while defence is a top priority for the EU (Mauro and Thoma 2016), the Commission views dual-use research as a solution for the lack of investment in research and innovation.

In 2014, the Commission proposed an industrial plan in the field of defence with the title *A New Deal for European Defence* expressed its intention to support CSDP-related research in three ways, one of which was dual-use research (European Commission 2014c). In order for this to happen, the EU recognizes that it needs to invest in defence research and development, and for that reason there has been a call to increase the 'dual use' research share of the Horizon 2020 budge phase (2018-2020). Under Horizon 2020 a total of € 164 million was allocated to 'dual use' technologies including Critical Infrastructure Protection, (2016 budget EUR 20 million), Security (2016 budget EUR 113.25 million), and Digital Security Focus Area (2016 budget EUR 29 million; figures provided in Mauro and Thoma, 2016). An additional push towards dual-use research came as the European Council invited Member States to increase investment in cooperative research programs and called on the Commission and the European Defence Agency (EDA) to develop proposals that would further stimulate dual-use research **(**European Parliament 2019).

Another important actor in the field of EU defence research is the EDA. There is continuous work on defence-related SMEs with a focus on dual-use activities and cross-border cooperation across the European defence supply chain. The support for dual-use is clearly illustrated in the EDA's activities. Since 2013, EDA has provided assistance for stakeholders in the defence sector to access ESIF co-funding for dual-use projects through various means such as raising awareness among defence stakeholders, providing coaching support for pilot projects, and developing a methodology (ibidem). In concrete, EDA's roadmap (EDA 2016) for dual-use technologies consists of the following elements:

- identifying and supporting dual-use Key Enabling Technologies (KETs),

- the development of nano-technologies through the public-private partnership Electronic Components and Systems for European Leadership Joint Understanding (JU ECSEL); and
- the research for dual-use technologies eligible for funding through Structural and Investment Funds

An important means through which the EU promotes research on dual-use technology is through the publication of detailed, step-by-step brochures where it reaches out to different potential recipients of the EU funding. In some cases, it is the Commission that issues theses guides, for example targeting SMEs and different regions (European Commission 2014b), other times it is the EDA (2015). Through its brochure "Your Guide to European Structural Funds for Dual-use technology projects", for example, the EDA (2015) provides a comprehensive document that breaks down the step-by-step process a defence actor should follow in order to secure dual-use funding, therefore incentivizing defence actors to access EU funding for the dual use technologies.

The arms control dimension

An important aspect of the political debates around dual-use technology refers to its arms control dimension. Precisely because they can also be used for military purposes, dual-use goods are subject to expert controls mechanisms, and within the EU the key document is the 2009 EU Dual-use Regulation (Council Regulation 428/2009), that establishes a common legal basis for member states' controls of the trade of these goods. The Regulation has different annexes, updated on a regular basis, that list the different dual-use technologies that are covered by the rules of said Regulation. These annexes follow closely the list of nine categories of dual-use goods covered by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[3]. In 2016 the European Commission published a proposal for recasting the regulation in order to provide it with a human security dimension and to cover certain

[3] These are the nine categories: (1) Special Materials and Related Equipment; (2) Materials Processing; (3) Electronics; (4) Computers; (5 - Part 1) Telecommunications; (5 - Part 2)"Information Security"; (6) Sensors and "Lasers"; (7) Navigation and Avionics (8); Marine; (9) Aerospace and Propulsion.

types of cyber-surveillance (Lavallée 2018). At the time of writing the three EU institutions involved in the recast process (Commission, Parliament, and Council) have not agreed on the terms in which the Regulation should be amended.

Seeing EU dual-use technology through an STS perspective

In the EU, member states have the main responsibility for providing security to their citizens. This crucial principle of competence allocation opens a somewhat different trajectory of security politics at the EU level. This idea, coupled with an understanding of security as a derivative concept — i.e., what 'security' is (or should be) is derived from one's political outlook and philosophical worldview (Booth 2007: 104–119) — implies that the definition of what counts/should count as a security issue for the EU is not provided by an external authority or a government, nor is it objectively defined. Rather, it results from a multi-layered process involving formal and informal decisions made by public and private actors, who create the knowledge base upon which policy decisions are made and priorities are defined.

In this context, the pursuit of technological knowledge in the security and defence realms becomes a political choice with relevant political consequences. Even if the European Commission frames much of the EU-funded dual-use research as being mostly an industrial policy – for example by promoting it to SMEs and regions, as illustrated above – these options do not fall outside the domain of politics; rather, they bring elements to claim a new centrality of technology in IR and security studies, because security technologies are "changing the way we conceive of foreign policy and security threats" (Martins 2019).

By promoting dual-use research as a way to reinforce EU defence R&D and advance industrial and innovation policies in the EU, the many EU actors involved in this process illustrate the above-mentioned shift in the understanding of the dual-use dilemma, i.e, a growing focus on the synergies and possibilities opened-up by these technologies, rather than on the risks they entail. This shift does not mean that risks are neglected. It means instead that the emphasis on the promise of dual-use technology reflects a strategy

through which the peculiar character of these technologies is used to advance an agenda that it industrial but also political.

To recover the expression of Molas-Gallart mentioned earlier, these technologies "can be used for instance, as a new, more palatable way of presenting measures of support to an industry that has lost some of its capacity to draw political backing" (Molas-Gallart 1997: 370). The provision qualifying 'dual-use' technology as eligible for receiving EU R&D funding through the SRP has been crucial for defence companies to receive EU funding while direct defence R&D funding was prohibited and to foster consortia and projects that developed 'security solutions' employing this type of technology.

Additionally, the shift in the understanding of the dual-use dilemma impacts the participatory governance of security concerns, which are often not sufficiently addressed at the EU level. This, in turn, affects the RRI principle and threatens to render inefficient the efforts in making it a central premise of security and defence R&D in the EU.

The concept of dual-use technology in the security and defence realms adds value to the broader theoretical and empirical discussion on (the blurring of) the distinction between security and defence, and between the civilian and the military domains. A clear illustration of the growing enmeshment of all these concepts deals with issues of spin off and spin on, that can be cogently understood by using theoretical concepts such as circulation, vouching for the necessity of further dialogue between intellectual traditions emanating from STS and critical approaches to security and military studies.

Conclusions

In the context of this volume, a deeper incursion on the concept of dual-use technology plays a very important role for two main reasons. Firstly, because the EU's engagement with security technologies happened mostly through fomenting, promoting, and funding dual-use technology, as demonstrated in this chapter. Secondly, and most importantly, civilian and military technologies are getting increasingly entangled, and therefore a clear separation of both domains is increasingly impossible to draw. Technology transfers between both fields are happening on a constant basis, and, most importantly, crucial

technology used in military contexts emerged from civilian and commercial contexts. Throughout the Cold War, many technological breakthroughs happened in the military context, and only afterwards were imported to the civilian sphere. Among these are nuclear energy, the internet, jet engines, missile technology leading to space craft, and the GPS navigation system, for example. Today, much of the technology used in military contexts is developed in the civilian and commercial sphere and further imported into the military sphere. Among examples of these technologies are face recognition tech, artificial intelligence, and swarm drones.

These technologies, which will play an important role in the conduct of political violence in the near future, are dual-use per definition. Understanding the broader societal and scientific debates surrounding dual-use technologies is therefore pivotal for understanding the politics surrounding its use.

References

Alic, J.A., Branscomb, L.M., Brooks, H., Carter, A.B., and Epstein, G.L. (1992) *Beyond Spinoff: Military and Commercial Technologies in a Changing World*. Boston, MA: Harvard Business School Press.

Alic, J.A. (1994). The Dual Use of Technology: Concepts and Policies. *Technology in Society* 16(2), 155–172.

Aradau, Claudia and Blanke, Tobias (2010). Governing circulation: A critique of the biopolitics of security. In: de Larrinaga, Miguel and Doucet, Marc G. eds. *Security and Global Governmentality: Globalization, Governance and the State*. London: Routledge

Atlas, R. M., & Dando, M. (2006). The Dual-Use Dilemma for the Life Sciences: Perspectives, Conundrums, and Global Solutions. Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, 4(3), 276–286.

Basham, V. M., Aaron Belkin & Jess Gifkins (2015) What is Critical Military Studies?, *Critical Military Studies* 1(1): 1-2.

Berling, T.V. and Bueger, C (2015) Security Expertise: Practice, Power, Responsibility, London: Routedge.

Bigo, D., Jeandesboz, J., Martin-Maze, M., and Ragazzi, F. (2014) *Review of Security Measures in the 7th Research Framework Programme*, Justice and Home Affairs (LIBE), Brussels: European Parliament.

Booth, K. (2007) *Theory of World Security*. Cambridge: Cambridge University Press.

Burgess, J.P. et al ed (2018) *Socially Responsible Innovation in Security: Critical Reflections*, Routledge.

Carmel, E. (2017) "Re-interpreting knowledge, expertise and EU governance: The cases of social policy and security research policy", *Comparative European Politics* 15(5): 771-793.

Ceyhan, A. (2012) "Surveillance as biopower", Ball, Kirstie, Kevin D. Haggerty, David Lyon eds, *Routledge Handbook of Surveillance Studies*, London: Routledge.

Cowan, R., and Foray, D. (1995). Quandaries in the economics of dual technologies and spillovers from military to civilian research and development. Research Policy, 24(6), 851–868.

Edler, J. and James, A. D. (2015) Understanding the emergence of new science and technology policies: Policy entrepreneurship, agenda setting and the development of the European Framework Programme, *Research Policy* 44 (6): 1252-1265.

European Commission (2019) *Secure societies – Protecting freedom and security of Europe and its citizens*. Available at: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-–-protecting-freedom-and-security-europe-and-its-citizens

European Commission (2014a) FP7-SECURITY - Specific Programme "Cooperation": Security. Available at: https://cordis.europa.eu/programme/rcn/861_en.pdf.

European Commission (2014b) *EU Funding for Dual Use. Guide for Regions and SMEs*. REF Ares(2015)3866477, DG Enterprise and Industry, Brussels: European Commission. Available at http://ec.europa.eu/DocsRoom/documents/12601/attachments/1/translations/en/renditions/native.

European Commission (2014c) A New Deal for European Defence, Brussels, 24.6.2014 COM(2014) 387 final. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede110914dealeuropeandefence_/sede110914dealeuropeandefence_en.pdf.

European Commission (2007) 'What is FP7? The basics', *FP7 in Brief*, available at: https://ec.europa.eu/research/fp7/understanding/fp7inbrief/what-is_en.html.

European Defence Agency (2016) *Dual-Use Research*. Available from: https://www.eda.europa.eu/what-we-do/activities/activities-search/dual-use-research.

European Defence Agency (2015) *Your Guide to European Structural Funds for Dual-use technology projects*, Brussels: European Defence Agency.

European Parliament (2019) *Fact Sheets on the European Union: Defence Industries*. Available at: https://www.europarl.europa.eu/factsheets/en/sheet/65/defence-industry.

Foucault, M. (2007) *Security, Territory, Population*. Basingstoke: Palgrave.

Gummett, P. ed. (1991) *Future Relations Between Defence and Civil Science and Technology*, Report for the UK Parliamentary Office for Science and Technology. London: Science Policy Support Group.

Hurlbut, B (2015) 'Remembering the Future: Science, Law, and the Legacy of Asilomar.', in S. Jasanoff and S-H. Kim (eds), *Dreamscapes of Modernity: Sociotechical Imaginaries and the Fabrication of Power*, Chicago: University Of Chicago Press: pp. 126-151.

James, A.D. (2018) 'Policy entrepreneurship and agenda setting: comparing and contrasting the origins of the European research programmes for security and defense', in N. Karampekios, I. Oikonomou and E.G. Caryannis (eds), *The Emergence of EU Defense Research Policy: From Innovation to Militarization*, Cham: Springer International Publishing AG, pp. 15–43.

Jeandesboz, J. and Ragazzi, F. (2010) *Review of security measures in the Research Framework Programme*, Citizens' Rights and Constitutional Affairs, PE 432.740, Brussels: European Parliament.

Kulve, H. T., & Smit, W. A. (2003). Civilian–military co-operation strategies in developing new technologies. *Research Policy*, 32(6), 955–970.

Lavallée, C. (2016) "La communautarisation de la recherche sur la sécurité: l'appropriation d'un nouveau domaine d'action au nom de l'approche globale", *Politique européenne*, no 51, 31–59.

Lavallée, C. (2018) "The EU's Dual-Use Exports: A Human Security Approach". in Pejsova, E. (ed) *Guns, engines and turbines*, Paris: EU Institute for Security Studies, pp. 43-50.

Leese, M., Lidén, K. and Nikolova B. (2019) 'Putting critique to work: Ethics in EU security research', *Security Dialogue* 50(1): 59–76.

Martins (2019) The global politics of security technologies, *Global Affairs* 5 (2): 105-106.

Martins and Küsters (2019) Hidden Security: EU public research funds and the development of European drones. *Journal of Common Market Studies* 57 (2): 278-297.

Molas-Gallart, J. (1997). Which way to go? Defence technology and the diversity of 'dual-use' technology transfer. *Research Policy*, 26(3), 367–385.

Molas-Gallart, J. (2002). Coping with Dual-Use: A Challenge for European Research Policy. *Journal of Common Market Studies*, 40(1), 155–165.

Owens, R., Macnaghten, P., & 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.

Pustovit, S. V., and Williams, E. D. (2008). Philosophical Aspects of Dual Use Technologies. *Science and Engineering Ethics*, 16(1), 17–31.

Rath, J., Ischi, M., & Perkins, D. (2014). Evolution of Different Dual-use Concepts in International and National Law and Its Implications on Research Ethics and Governance. *Science and Engineering Ethics*, 20(3), 769–790.

Resnik, D. B. (2010). Can Scientists Regulate the Publication of Dual Use Research? *Studies in Ethics, Law, and Technology*, 4(1).

Rychnokská, D. (2016) Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security, *Security Dialogue* 47(4) 310–328.

Selgelid, M. J. (2009). Dual-Use Research Codes of Conduct: Lessons from the Life Sciences. *Nanoethics* 3 (3).

Stavrianakis, A. and M. Stern (2018) Militarism and security: Dialogue, possibilities and limits, *Security Dialogue* 49(1-2) 3–18

Stilgoe, J. and Guston DH (2017) 'Responsible Research and Innovation', in Felt, U. et al eds, *Handbook of Science and Technology Studies*, Cambridge, MA: The MIT Press.

Verbruggen, M. (2019) 'The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems', *Global Policy* 10 (3): 338-342.

Vogel et al (2017) 'Knowledge and Security', in Felt, U. et al eds., *The Handbook of Science and Technology Studies*, MIT Press, 973-1001.