Technological Expectations and the Making of Europe

Jens Hälterlein

Department of Media Studies, Paderborn University, Germany/
jens.haelterlein@upb.de

Abstract

In a case study approach, the paper traces how technological expectations have been influential in the creation of European institutions, R&D programmes and regulatory instruments and how they have contributed to processes of European integration. The first case study shows how the promises of a coming 'Atomic Age' have been mobilized to support the foundation of the European Atomic Energy Community and, thus, contributed to European integration in the post-WW2 era. The second case study analyses how the security stream within the EU's framework programmes for R&D is shaped by the promise of 'technosecurity' and enacts the normative claim of the EU's security integration in the post-Cold War era. The third case study analyses how the EU's AI strategy and AI act articulate the vision of a 'human-centric AI' and how this vision is related to the EU's current attempt to restore citizens' trust in times of crisis.

Keywords: Europe, Technological Expectations, Nuclear Power, Security Technologies, Artificial Intelligence

Introduction

The future of the 'European project' has frequently been addressed as a question of developing and regulating new and emerging technologies that are at once praised as a driver of progress and seen as a major source of problems. In the post-WW2 era, nuclear power fuelled the hope to replace all other power sources and ultimately lead Europe into an age of peace and prosperity. In its weaponized form, however, it became an existential threat to Europe being a likely battlefield of a nuclear war. In the post-Cold War era, digital infrastructures and Information and Communication Technologies (ICTs) became the lifelines of Europe's high-tech societies and at the same time a source of their susceptibility to cyberattacks, natural disasters, major accidents and highly contagious diseases. Recently, Artificial Intelligence (AI) has been imagined as a panacea for all kinds of societal grand challenges and as a multifaceted threat to the fundamental rights and even lives of the citizens of the European Union (EU).

In order to take advantage of the opportunities, these technologies create and control the risks they entail, their development and regulation have become problems that a European government and politics have to address. As they mobilized and legitimized activities and resources they contributed to the formation of governance of science, technology and innovation (ST&I) on a European level (Barry, 2001). However, the fears and promises associated with these technologies not only sparked the definition of rules and undertaking of measures to push ahead innovation or restrict their use. They also functioned as a crucial component of endeavours to advance the 'European project'. Within these endeavours, technologies became 'Europe-building tools', instruments of connection either creating unifying themes for national policies or new challenges that could only be addressed collectively.

The purpose of this paper is to acknowledge how European integration after WW2 was and is connected to technologies that figure both as objects of political intervention and as media for the construction of a political community. In a case study approach, the paper traces how technological expectations have been influential in the creation of European institutions, R&D programmes and regulatory instruments and how they have contributed to processes of European integration. The first case study shows how the promises of a coming 'Atomic Age' have been mobilized to support the foundation of the European Atomic Energy Community (EURATOM) and, thus, contributed to European integration in the post-WW2 era. The second case study analyses how the security stream within the EU's framework programmes for R&D is shaped by the promise of 'technosecurity' and enacts these promises in a way that reflects the normative claim of the EU's security integration in the post-Cold War era. The third case study analyses how the EU's AI strategy and AI act articulate the vision of a 'human-centric AI' and how this vision is related to the EU's current attempt to restore citizens' trust in times of crisis. The following section discusses the two relevant research strands on the topic and presents the central findings of the paper.

Connecting technological expectations and European integration in a historical case study approach

Expectations in science and technology have been studied under various terms such as technoscientific promises, technophobia, guiding visions ('leitbilder'), and (sociotechnical) imaginaries (for an overview, see: Konrad et al., 2017). These expectations can have a range of effects in the context of R&D, ST&I policies and public engagement. By promising future economic success, they can attract investments from private and public actors (Beckert, 2013). They can serve as epistemic orientation and coordination in heterogeneous innovation networks by pre-selecting design options and synchronizing expectations (Fujimura, 2003). They influence the acceptance or rejection of technologies among users and the general public (Brown et al., 2000). And they legitimize or delegitimize the actions of public authorities such as the funding of national R&D programmes, investments in material infrastructures and legislative initiatives (Jasanoff and Kim, 2009). While technological expectations and their effects have been studied in numerous contexts and with various scopes, their role in the creation of political communities and the imagination of nationhood has received comparatively little attention, especially with regard to the European project (see, for instance: European Commission and Directorate-General for Research and Innovation, 2007 and Mager, 2017).

Investigating the technological dimension of European integration places this paper in the tradition of another research strand. Scholarship on the history of technology[1] has shown that transnational infrastructures, material networks and the circulation of knowledge and artefacts have shaped European identities in a bottom-up "hidden integration" process starting in the 1850s (Misa and Schot, 2005: 2). Moreover, it has been proposed to view certain technology developments and large-scale technological projects "as a set of Europe-building practices in which specific concepts and visions of Europe became embedded in particular designs for artefacts and systems" (Misa and Schot, 2005: 9). This research strand investigates the co-production of technology and Europe by means of what Gabrielle Hecht (1998: 15) has labelled *technopolitics*: "the strategic practice of designing or using technology to constitute, embody, or enact political goals". While scholarship from the history of technology has focussed on the technopolitics of producing, standardizing and using technologies, infrastructures, products and expertise, the technopolitics of mobilizing and addressing expectations in science and technology has received far less attention.

Connecting both research strands, this paper presents three cases that exemplify how technological expectations have shaped European integration processes after WW2.

The case studies primarily draw on in-depth analysis of European policy documents – statements, reports, communications, treaties, and legal texts. All of them are publicly available via online repositories. These documents are the result of complex negotiation procedures between various actors which are, however, outside the scope of this paper. In addition, the case studies integrate research findings on various individual aspects of the topics that have been produced in STS and adjacent disciplines. Even though the aim of this paper is not to produce a comprehensive account of the history of European integration, the insights it provides go beyond the individual cases. Together, the three cases display shifting strategies to advance European integration and different meanings of the European project. But they also display a constant preoccupation of European government and politics with the problems technology poses and with the potential benefits it promises. Moreover, the paper reveals recurrent themes that prevail throughout the cases: the security-technology-nexus, the problem of constructing a single market for technologies and the need to address their potential dual-use. Combining historical and contemporary cases, thus, enables us to reflect the simultaneity of continuity and discontinuity in the making of Europe.

The 'Atomic Age' - nuclear power and European integration in the post-WW2 era

The end of WW2 not only marked a rupture in European history but also heralded the 'Atomic Age'. Advancement in harnessing the power of atoms created new, ambivalent relationships among science, technology and society. On the one hand, these advancements led to the development of nuclear weapons whose destructive power has been demonstrated to the world with the bombings of Hiroshima and Nagasaki. These events not only led to the unconditional surrender of Japan but were also catalysts for a 'Cold War' arms race that culminated in the antagonistic conflict of two superpowers equipped with weapon arsenals of unprecedented destructiveness. The notion of 'nuclear exceptionalism' was cultivated to indicate both the exceptional nature of this human creation and the exceptional global power of the U.S. and the Soviet Union (Hecht, 2006). Consequently, the decision to build or possess nuclear weapons may not only follow security and defence considerations but also serve the symbolic purpose of demonstrating national strength and greatness. Becoming a nuclear weapon state, thus, shapes and is shaped by a state's national identity (Sagan, 1996). For anti-nuclear activists and engaged scientists, however, the mere possibility of a first (or pre-emptive) strike carried out by one of the nuclear powers, no matter how likely or unlikely, revealed that technoscience is producing risks of vital scope. The dystopian imaginary of a 'nuclear apocalypse' that could consume all life on the planet stood as a symbol of a society that creates the powers of its annihilation. It sparked the creation of popular culture, mobilized nuclear disarmament movements and led to the implementation of nuclear civil defence systems in the U.S., the Soviet Union and almost all countries of Western Europe (Cronqvist et al., 2022). On the other hand, the peaceful use of nuclear power was celebrated as the solution to the problem of securing a sufficient energy supply for the growing national economies. The origins of this promise can be traced back to the early days of research on radioactivity (Weart, 2012). After WW2, the U.S.' Atoms for Peace campaign, as well as international conferences, science exhibitions and media representations publicly promoted nuclear power as the ultimate solution to future energy problems (Spiering, 2011; Trischler and Bud, 2018). Nuclear energy was expected to replace all other power sources and ultimately lead to an age of peace and prosperity for humankind since it would "provide the power needed to desalinate water for the thirsty, irrigate deserts for the hungry, and fuel interstellar travel deep into outer space." (Sovacool, 2011: 259) The imaginary of a coming 'Atomic Age' as a desirable future equated the peaceful use of nuclear power with progress and modernity per se. It sparked the imagination of inventors and policymakers alike, leading to the development of food irradiation and nuclear medicine and legitimizing research funding for the development of nuclear-powered cars and aircraft.

For the two superpowers as well as many countries both in Europe and on the 'nuclear periphery', the development and regulation of nuclear energy offered the possibility to secure economic progress, demonstrate technological prowess, and present themselves as guided by rational, scientific means (Hecht, 1998, 2006; Jasanoff and Kim, 2009; Kaijser, 2021; Richers et al., 2018; Welsh, 2000). At the same time, developing or being in the possession of nuclear weapons became the ultimate signature of the geopolitical status of a nation (Hecht, 2006). For the making and shaping of Europe, 'nuclear identity' has been no less important. The promises of a coming Atomic Age influenced the articulation of a vision of Europe that rested on the classical modern understanding of progress as a marker of the ties between science and the state. It portrayed a „European government that was based on the advanced areas of scientific research and justified by the increasing economic demands of science." (Barry and Walters, 2003: 310) This entanglement of Big Science with early post-WW2 politics was different from the one in the U.S., the Soviet Union, the U.K. and France where publicly funded nuclear research was connected to both, nuclear energy and nuclear weapons development (Hecht, 1998; Holloway, 1994; Krige, 2016; Rhodes, 1988; Richers et al., 2018; Welsh, 2000). By drawing a dividing line between the military and the civil use of the atom, between the utopian and the dystopian elements of the 'Atomic Age', European integration was envisioned as a result of cooperation in the nuclear energy sector only.

Due to the geopolitical constellation that placed Europe at the centre of the "Cold War' it was widely expected that the continent would be turned into a battlefield in case of a clash of the two superpowers (Spiering, 2011: 171). Therefore, nuclear deterrence played a fundamental role in keeping peace and preserving stability on the continent. As part of the North Atlantic Treaty Organisation (NATO) strategy of Western defence integration and nuclear deterrence policy, both land- and air-based delivery systems of the U.S. Army were deployed in the U.K., France, Belgium, Germany, the Netherlands, and Italy since the 1950s. For most of the European NATO members, nuclear deterrence rested on the U.S. (except for Britain and France). Only two Western European states successfully developed their own nuclear deterrent – Britain in 1952 and France in 1960. While the British nuclear programme benefited strongly from U.S. aid and consequently led to a status where its nuclear forces were fully integrated into the nuclear defence strategy of the NATO, France used its nuclear weapons (the 'force de frappe') to gain the ability to distance itself from NATO and to defend France even if the U.S. refused to assist in the event of a Soviet nuclear attack or invasion. On the contrary, an integrated deterrence under the collective control of Western Europe (as a result of the 'Europeanisation' of the French nuclear deterrence) never became a real option (Sauer, 2020).[2] This dependency in the field of nuclear deterrence was symptomatic of the failure of European security and defence integration during the 'Cold War'. In 1954, an early attempt to create a European Political Community (EPC) – envisioned as a combination of the existing European Coal and Steel Community (ECSC) and the proposed European Defence Community (EDC) – failed after the French National Assembly refused to ratify the Treaty establishing the EDC which proposed the creation of a European army at the disposal of the EDC.

However, already in June 1955, the foreign ministers of the six member-states of the ECSC proposed „to take a new step on the road of European construction" (Commission of the European Communities, 1955: 2) through both 'horizontal' integration by establishing a common market and 'vertical' integration in the transport and energy sector. Besides securing the supply of conventional energy, one of the objectives defined in the *Messina Declaration* was the „development of atomic energy for peaceful purposes" which "will very soon open up the prospect of a new industrial revolution beyond comparison with that of the last hundred years" (Commission of the European Communities, 1955: 2). Here, the *Messina Declaration* used the high expectations regarding nuclear energy to call for a collective endeavour. This endeavour, however, would necessarily imply a transfer of power from the nation states to a new European institution: Sectoral integration in the field of nuclear energy would require „the creation of a joint organization to which will be assigned the responsibility and the means to secure the peaceful development of Atomic Energy" (Commission of the European Communities, 1955: 2). With the creation of the *European Organization for Nuclear Research* (CERN) in 1953 and the *European Atomic Energy Society* (EAES) in 1954, two joint organizations had already been established. However, the missions of both organizations were limited to research cooperation. While the CERN was supposed to create a European laboratory for basic research in nuclear and particle physics, the EAES was supposed to facilitate exchange on civil nuclear energy research by organizing meetings for scientists and engineers working in the field (European Atomic Energy Society, 1954). The objectives of nuclear energy integration as envisioned in the *Messina Declaration* and the *Spaak Report* (Comité intergouvernemental créé par la conférence de Messine, 1956) would go beyond research cooperation and would also include common investments and joint ventures, the centralized supply of the member states with ores and nuclear fuel, a common market for materials, tools and special equipment, and a new European organization with exclusive competences in nuclear energy matters and far-reaching supervisory powers.[3] This new organization would operate under the name *European Atomic Energy Community* (EURATOM).

There was ample reason to believe in the success of this endeavour. Being a technology under development, nuclear energy was perceived as an unregulated field of S&T policy (Barry and Walters, 2003: 309). Thus, there was hope that common efforts in the nuclear energy sector would not have to deal with established national interests and could gain the benefits of collaboration in scale. Moreover, in its nascent stage, EURATOM was strongly supported by the U.S. since a regional organization for the promotion of civilian nuclear power in Europe was perceived as a focal point for the extension of the "Atoms for Peace" program beyond research.[4] In the eyes of the State Department and the Secretary of State John Foster Dulles, "nuclear science and technology provided the material infrastructure that would help bind the U.S.'s continental allies together" (Krige, 2008: 7). A second important assumption in favour of sectoral integration in the nuclear energy field was that necessary investments in infrastructure (including a steady supply with raw materials) and technology of nuclear R&D were so cost-intensive that they exceeded the financial capabilities of medium and small states of Western Europe. Therefore, the pooling of financial resources, industrial capacities and varied skills seemed to be the only way to let the promises of the peaceful use of the atom come true. This argument was first brought up in a report for the OEEC, commissioned in early 1954 and published in June 1955. The report predicted that „[n]uclear energy gives Europe the possibility of having an abundant supply of power at steadily decreasing cost in 15 or 20 years' time" (Armand, 1955). However, „as many Member countries do not seem to dispose of the means required for carrying out a nuclear programme and there are a great many technical problems the solution of which will call for a co-ordinated effort backed by the mobilised industrial potential of all Member countries." (Armand, 1955) Finally, a third factor played into the hands of those political forces in favour of a collective effort in nuclear energy production: the perceived scarcity of fossil fuels at that time. In October 1956, the Ministers of Foreign Affairs of the six ECSC member states commissioned a report "on the amounts of nuclear energy which can be produced in the near future in the six EURATOM countries, and the means to be employed for this purpose" (Armand et al., 1957: 13). The report entitled *A Target for EURATOM* highlighted the lack of significant coal deposits in Europe as well as the extent to which the ECSC countries were already dependent on oil from the Middle East. Moreover, it anticipated a growing need for energy over the next few years as requirements would double in ten years and treble in twenty. Therefore, any interruption of oil supplies would imply tremendous risks. Accordingly, the report recommended the replacement of power stations running on coal and oil and the creation of a nuclear sector producing competitively priced electricity:

> if our countries, guided and stimulated by EURATOM, make the necessary effort they will in future command - as the New World does now - abundant and cheap energy supplies, enabling them to enter boldly into the atomic era. (Armand et al., 1957: 17)

With the Treaty of Rome, signed in March 1957, EURATOM was established along with the EEC. Re-articulating the promises of the 'Atomic Age', the preamble of the Treaty establishing EURATOM states "that nuclear energy represents an essential resource for the development and invigoration of industry and will permit the advancement of the cause of peace" (EURATOM, 1958). The promise of energy security, however, was attached to a vision of Europe as the preamble expresses the conviction "that only a joint effort undertaken without delay can offer the prospect of achievements commensurate with the creative capacities of their countries" (EURATOM, 1958). Accordingly, the primary tasks of the nuclear energy community are "to contribute to the raising of the standard of living in the Member States […] by creating the conditions necessary for the speedy establishment and growth of nuclear industries" (EURATOM, 1958: 13). In order to perform this task, the Community shall undertake actions to ensure a regular and equitable supply of raw materials as well as commercial outlets and access to the best technical facilities (Article 2). For the former action, a EURATOM Supplies Agency (ESA) was to be created that would own and control the supply of all fissile materials in the Community. For the latter action, the Community shall create a common market for special materials and ensure free movement of capital for investment and freedom of employment for specialists in the nuclear energy sector. Furthermore, the Community is to "promote research and ensure the dissemination of technical information" (Article 2). Besides the promotion of nuclear research in the Member states, community research and training programmes and *Joint Nuclear Research Centre* were to be set up (Articles 4 and 8).

While the primary mission of EURATOM was the promotion of a nuclear industry within the Community, its secondary mission was the regulation of this industry. Accordingly, the Treaty defines measures by which the risks associated with the peaceful use of the atom should be governed. On the one hand, the Community declared to satisfy itself that "ores, source materials and special fissile materials are not diverted from their intended uses as declared by the users" (Article 77). The Treaty introduces a system of safeguards designed to ensure that civil nuclear material is not diverted for military purposes. However, the Treaty neither prohibits nor explicitly permits the possession of nuclear weapons. This was a sine qua non for the inclusion of France which was pursuing its nuclear weapons program at that time and threatened a veto if the treaty would include such a prohibition clause. On the other hand, EURATOM aimed to establish and apply uniform safety standards for the protection of the health of workers and the general public against the dangers arising from ionizing radiation.

At the time of its adoption, EURATOM was seen as a progressive and charitable endeavour centred on promoting the collective development of a civil nuclear industry in Europe. However, while the CERN is acclaimed to be the model of successful European cooperation (Lalli, 2021; Mobach and Felt, 2022), this is not the case with EURATOM which is widely considered to have failed (Wolf, 2011) mainly for three reasons. Firstly, EURATOM wasn't able to coordinate national efforts in nuclear R&D. Eventually, national interests prevailed and the member states used higher funds for their national nuclear energy programs than they made available to EURATOM (Commission of the European Communities, 1968: 13). Secondly, contrary to the pessimistic forecasts preceding the EURATOM Treaty, global oil reserves proved to be sufficient due to the discovery of new deposits in the Global South, the expansion of production in the Soviet Union, and offshore production in the North Sea. Thirdly, the promises of a coming 'Atomic Age" lost their persuasiveness with nuclear energy increasingly being problematized both in terms of the possibility of nuclear accidents with disastrous consequences and in terms of the risks deriving from the handling and storage of nuclear waste.

The historical relevance of EURATOM, however, should not only be judged by its failure to create an integrated European nuclear industry. EURATOM embodied a vision of the European project that highlighted sectoral integration in the field of nuclear energy production as a necessary complementary approach to the project of a common market since an adequate supply of energy was imperative to sustain economic growth and political stability (Krige, 2006). In the period preceding the ratification of the Treaty of Rome, it was widely believed that EURATOM "held the greatest promise of success, while the EEC negotiations faltered" (European Parliament, 2002: 12). Moreover, the pairing of the two European Communities is considered as a "crucial factor in initially persuading and eventually convincing a sceptical French Government to engage with European integration after the embittering experience of the aborted European Defence Community" (European Parliament, 2002: VII). Therefore, the political radiance of EURATOM has been no less than the one of the CERN and other Big Science collaborations in Europe (Cramer, 2020). At a time when the 'Atomic Age' could still be understood in a positive, futuristic sense and a European identity was (even more than it is today) a fragile construct, the promises of a collective endeavour in nuclear energy production became a catalyst for European integration after WW2.

'Technosecurity' - European security research and security integration in the post-9/11 era

While the EURATOM treaty is still in force and nuclear energy is accounting for about one-fourth of the electricity produced in the EU, the promise of nuclear power to provide the ultimate means for peace and security has become even more controversial in the aftermath of the 1986 Chornobyl and the 2011 Fukushima disasters. With regard to the EU's objective to reach climate neutrality by 2050, most member states classify nuclear power as a 'clean energy' while some strictly oppose this view. The fear of Europe becoming a nuclear battlefield, on the other hand, lost ground after the fall of the iron curtain while at the same time a new imaginary of (in)security emerged that runs contrary to the categorical distinction between domestic and military security. The security of Western nation-states and their populations no longer appeared to be threatened by a clearly identifiable military enemy, but by a heterogeneous spectrum of threats, ranging from terrorism to transnational organized crime, large-scale disasters, illegal migration, and the spread of viruses throughout physical and virtual space. These multi-faceted, dynamic factors are seen as globalized insecurities of an increasingly globalised world, in which the circulation of people, goods, information and risks does not stop at national borders (Beck, 1998). Therefore, the post-Cold War security policies are addressing the ambiguity of the technological constitution of a physical and virtual network society (Dillon, 2002): digital infrastructures and Information and Communication Technologies (ICTs) are considered to be the lifelines of high-tech societies and at the same time a source of their susceptibility to cyberattacks, natural disasters, major accidents and highly contagious diseases (van der Vleuten et al., 2013). As 'vital systems" they simultaneously foster new forms of vulnerability (Lakoff and Collier, 2010). Moreover, they enabled the formation of international terror networks. The same line of thinking applies to the technoscientific achievements of modernity in general. They are treated as both, targets that need protection and veritable threats to security. As Langdon Winner has put it: "The horror of the World Trade Centre attack was that the power of two wonders of modern technology – the skyscraper and the jet airliner – came crashing together causing the carefully contained power of both systems to be released in catastrophic explosion, inferno and collapse." (Winner, 2004: 166)

At the same time, however, technologization is praised as the new silver bullet for security issues (Aas et al., 2009; Ceyhan, 2008; Marx, 2001). Legitimized by the sheer complexity, diversity and interconnectedness of tasks – such as fighting terrorist networks, organized crime and illegal migration, cybersecurity, public health, disaster management, and critical infrastructure protection – and driven by the technoscientific promises of a growing security industry, the use of advanced technologies is becoming (or is supposed to become) a key element of security practices in various contexts. According to this new "technosecurity paradigm" (Mattelart, 2010: 137), there seem to be technological fixes for all security issues: facial recognition that identifies search-listed criminals and terrorists in real-time (Möllers and Hälterlein, 2013), body scanners and other sensory devices that detect weapons and dangerous substances at airports (Leese, 2015); satellite images and biometric passports that enable efficient border management; software that forecasts places and times of future crimes (Hälterlein, 2021); ICTs that enable efficient coordination of emergency and crisis response activities (Hälterlein et al., 2017) etc. In terms of security, technology, thus, is a double-edged sword: its omnipresence in western societies is considered to be one of the main causes of insecurity. At the same time, the deployment of security technologies is promoted as the ultimate solution for security authorities "to address our present problems and fears" (Bigo and Carrera, 2005: 3).

However, the promise of 'technosecurity' not only had an effect on security work but created new impulses to European integration as well. Already through the Maastricht Treaty of 1992, the Member States of the EU agreed on cross-border operational cooperation in dealing with their internal security challenges, consisting of judicial cooperation in criminal matters and cooperation of law-enforcement and border-management agencies. With the Amsterdam Treaty of 1997, security measures were grouped under the heading of the *area of freedom, security and justice* (AFSJ) "in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime" (European Union, 1997: Article 1(5)). However, in face of the common threats and challenges „of the dynamic and global twenty-first century" (Council of the European Union, 2010: 3–4) that are „cross-border and cross-sectoral" and therefore „go beyond our national, bilateral or regional capability" (Council of the European Union, 2010: 3–4), a more integrated approach was deemed necessary. Under the umbrella of the AFSJ, a new type of cooperative policy activity at the European level emerged in the post-9/11 era that „crosses sectoral boundaries, draws in a number of governmental and societal actors, and comprises a variety of institutional venues" (Boin et al., 2006).

To a large extent, this cooperative security policy is shaped by the promise of 'technosecurity'. Driven by the expectation that technological measures would provide security in the EU, numerous databases and information-sharing systems have been implemented: the European Dactyloscopy (EURODAC) in 2003, the Europol Information System (EIS) and the Customs Information System (CIS) in 2010, the European Criminal Records Information System (ECRIS) in 2012, and the European Border Surveillance System (EUROSUR) in 2013. While the implementation of these systems aims at integration and interoperability of national security practices through digital technologies and data infrastructures, a strong focus has been placed on fostering innovation by including civil security research in the Joint Research and Development Programme of the European Commission. Due to its exclusively civilian nature, the European Security Research Programme (ESRP) does not include direct funding for defence and military technology. Yet, it enables funding for dual-use technology that can be applied for both civilian and military purposes.

First steps towards establishing the ESRP as a new field of European security cooperation were taken with the creation of the *Group of Personalities on Security Research* in 2003, the *European Security Research Advisory Board* in 2005[5] and the launch of the *Preparatory Action on Security Research* in 2004. Eventually, security research was implemented within the 7th Framework Programme for Research, Technological Development and Demonstration (FP7) in 2007 with a proportional budget of EUR 1.25 billion. The Security theme of FP7 was conceived as a mission-oriented programme, addressing four main security challenges: Security of citizens, Security of infrastructures and utilities, Intelligent surveillance and border security, and Restoring security and safety in case of crisis (European Commission, 2015: 1). Since then, funding has increased continuously in terms of budget and scope. In the 2014 to 2020 period, the Horizon 2020 programme has allocated some EUR 2 billion to its 'Secure Societies' pillar which is about 50% of all public financing for security research in the EU. Research and innovation are carried out by consortia projects that enact a cross-border collaboration of policy-makers, security practitioners, the security industry and academia or by the EC's Joint Research Centre (JRC). The majority of the hundreds of projects that have been funded under the European Commission's Preparatory Action for Security Research, FP7 and Horizon 2020 focused on technical solutions "needed by those on the front line who must deal with terrorism, cybercrime, firearms, human trafficking and natural disasters." (European Commission, 2018d: 27)

Several arguments have been put forward justifying the ESRP instead of exclusively relying on national R&D programmes of EU member states or even non-EU providers. Firstly, pooling resources at the EU level is expected to generate added value, since it „facilitates finding solutions much faster and more efficiently compared to what can be done at national level." (European Commission, 2017: 29–30). EU funding for cross-border collaboration would generate synergies by breaking down the fragmentation across Europe's security sector and national markets. For European transnational corporations, there are high barriers to EU-wide market entry since the market for security products does not function as a 'single' EU market yet. It is fragmented into national markets with nation-specific demands driven by the nation-specific requirements of the respective public authorities, technical standards, and public procurement rules. This makes economic growth and market expansion difficult for the European security industry (European Commission, 2004). The problem of constructing a single market has been virulent in debates on European Integration during the 1980s and 1990s. Against the backdrop of cross-border security threats, market fragmentation is perceived as a source of vulnerability that has to be tackled. Therefore, establishing "a better functioning Internal European Market for security technologies" (European Commission, 2012: 3) through EU-wide standards and harmonized certification schemes is one of the main objectives both of the EU's security industry policy and the security research pillar of the framework programmes. In the same vein, the security research programme strongly supports the interoperability of the technological solutions and tools to be delivered, and specific intellectual property rights rules for security research as well as pre-commercial procurement. These measures are deemed to play a crucial role in creating a single market for security products and enabling Europe's security industry to create economies of scale, thereby contributing to the improvement of both Europe's security and the competitiveness of its security industry in global export markets (European Security Research and Innovation Forum, 2009).

Secondly, integrating security research in its Joint Research and Development Programme enabled the Commission „to define the technological capabilities required by the Union to carry out its common internal security policy, and to define the priorities in that area" (Citi, 2014: 136). It underpinned the EU's claims in the highly sensitive area of security where nation-states are particularly hesitant to give up their prerogative of having the main responsibility for providing security to their citizens. As part of this agenda setting, the Commission has set the requirement for research projects to take into account that security technologies "might directly or indirectly concern fundamental rights, such as the rights for respect for private and family life, protection of personal data, privacy or human dignity" (European Commission, 2012, 2014). Such an infringement of rights may lead to a lack of acceptance which is framed as the "societal dimension" (European Commission, 2012: 4) of security technologies. This societal dimension is associated with the risks of wasted investment in technology development and the need to rely on less controversial products which may not entirely fulfil security requirements (European Commission, 2012: 5). In order to address this problem, the European Commission calls for a "better integration of the societal dimension, by thoroughly assessing social impacts including impacts on fundamental rights, and by creating mechanisms to test the societal impact during the R&D phase" (European Commission, 2012: 5). Consequently, for all Horizon 2020 security research projects, an ethics review and a societal impact assessment (SIA) has become mandatory (European Commission, 2013).[6] Under the ELSA label (Hilgartner et al., 2017), research into **e**thical, **l**egal and **s**ocietal **a**spects of security technologies has been conducted either as part of R&D projects or within projects with a general focus on the "societal dimension" of security technologies. The concerns, identified by these "screening[s] of a project's ethical implications" (European Commission, 2016b: 26) are then to be translated into technological requirements. This translation process that first and foremost ensures compliance with data protection legislation by addressing privacy impacts of security technologies proactively, is summarized under the concept "privacy by design". According to this concept, technologies should be designed with privacy in mind from the outset of the innovation process, integrating privacy-enhancing features, most prominently so-called Privacy-Enhancing Technologies (PETs), into systems design. Ultimately, this approach would enable measures to prevent a lack of acceptance of security products.

Driven by the promise of 'technosecurity', the joint development of security technologies was used the drive forward European security integration: on the one hand by establishing a single market for security products by creating harmonized standards and schemes for security technologies and procurement processes, on the other hand by ensuring the interoperability of technological innovations that enable security practitioners from different Member States and EU organisations to operate together effectively. Hence, the ESRP underpins and enacts the vision of a 'Security Union' that has been articulated in the context of the renewed Internal Security Strategy of 2015 (European Commission, 2015). In a 'Security Union', the member states would agree on a shared responsibility and "move beyond the concept of cooperating to protect national internal security to the idea of protecting the collective security of the Union as a whole" (European Commission, 2016a: 2).

Moreover, a specific normative claim of the EU's security policy is inscribed into the operations and outputs of security research. Through the assessment of societal impacts at an early stage and the design-in of identified privacy implications, security research is supposed to create the means to push the boundaries of the so-called trade-off between security and privacy (Pavone and Degli Esposti, 2012) and offer a way out of the dilemma to choose between "effective intrusiveness and non-intrusive inefficiency" (Bigo and Jaendeboz, 2010: 6). The EU's internal security policy, hence, reflects and performs the dictum that security and respect for fundamental rights including privacy are not to be seen as conflicting aims, "but consistent and complementary policy objectives". (European Commission, 2015: 3) Against the backdrop of the vision of Europe as a union based on values (European Union, 2007, Article 2), the promise of 'technosecurity' nourish the promise of the AFSJ "that law enforcement measures, on the one hand, and measures to safeguard individual rights, the rule of law and international protection rules, on the other, go hand in hand in the same direction and are mutually reinforce" (European Council, 2010: 4). However, as the ongoing deadly events on Europe's external borders demonstrate in a terrifying manner, this area is a highly restricted area where security integration correlates with the exclusion of those human beings labelled as illegal.

A 'human-centric AI' – the EU's approach to building up trust in times of its crisis

The promise of 'technosecurity' continues to play a crucial role in Europe's internal security policy and its current R&D framework programme "Horizon Europe" (2021 – 2027). This is not likely to change with the Covid-19 pandemic as it has demonstrated the vulnerability of an interconnected world where infection dynamics take the speed of international mobility and put the security of citizens, the management of borders and the protection of critical infrastructures at the top of political agendas. Given the persuasiveness of technological solutions, digital contact tracing, computer simulations of propagation scenarios and syndromic surveillance systems are at the forefront of the fight against the spread of the virus. However, the pandemic has also fed into the current hype of AI and the imaginative powers it unfolds. AI is not only used to analyse the virus' genetic information and its mutations as well as to develop and test vaccines. It is also expected to provide the means to prevent future pandemics by predicting outbreaks based on the real-time analysis of vast amounts of heterogeneous data.

AI has always evoked diverse scientific, artistic and political visions. Utopian imaginaries of social progress through AI (Minsky, 1986; Moravec, 1995) contrast with dystopian imaginaries of AI as the hubris of the human mind (Weizenbaum, 1976). One of the currently most virulent AI-related fears is surely the one of AI as a 'job killer', given the possibility that advancements in AI-based production systems will lead to mass unemployment. Moreover, AI is under public scrutiny for causing deadly car accidents, enabling more invasive surveillance of citizens, more powerful cyberattacks on critical infrastructures, reproducing or even reinforcing discrimination in various societal contexts and being used to manipulate political opinion. Furthermore, the *Campaign to Stop Killer Robots* has demanded an international ban on lethal autonomous weapon systems (LAWs). At the same time, AI is praised as a key technology that enhances our capabilities to deal with societal grand challenges, for example by improving healthcare and cybersecurity, enabling a more sustainable economy, a cleaner and safer mobility, a more efficient food system and a smarter crisis management. Moreover, robots and other "smart machines" could replace difficult, dirty, dull or dangerous tasks in the context of care work, manufacturing, policing and emergency response. These technoscientific promises of AI have been initially articulated by private tech companies and other actors who are directly involved with the development and implementation of these technologies.

Recent advances in the AI-subfield of machine learning that is already used in many real-life applications, however, have made AI a matter of concern not only for futurist thinking, criticism or marketing but also for policymaking. In the past few years, many governments and supranational organisations published strategy papers in which they present their visions of the future development, application and regulation of AI. In 2016, the US presented their *National Artificial Intelligence Research and Development Strategic Plan* defining the government's role predominantly as a facilitator of innovation. The *National Artificial Intelligence Initiative* of 2019 emphasised the importance of continued U.S. leadership in AI R&D. China, on the contrary, plans to use a state-driven development model as part of its *Next-Generation Artificial Intelligence Plan*, which was presented in 2017 and sets the goal to become the global leader in the field of AI by 2030.

The EU entered into the policy field in 2017 with the European Parliament's Committee on Legal Affairs' resolution on *Civil Law Rules on Robotics* (European Parliament, 2017). Besides recommending several legislative initiatives, the resolution also calls on the European Commission to establish ethical guidelines to be respected in the development, programming and use of robots and AI. The European Commission soon took action by presenting a set of ethical principles for the development of *Artificial Intelligence, Robotics and 'Autonomous' Systems* (European Commission et al., 2018), its strategy *AI for Europe* (European Commission, 2018a) and the *Coordinated Plan on Artificial Intelligence* (European Commission, 2018b, 2018c) in 2018. In its strategy, the European Commission articulates the vision of a 'human-centric AI' as it claims to use the „power of AI at the service of human progress" and to benefit „people and society as a whole" (European Commission, 2018a). Instead of manipulating or replacing people and threatening their fundamental rights or even lives, AI should improve the lives of EU citizens through innovations in sectors such as health, farming, education, employment, energy, transport and security. In order "to make the most of the opportunities offered by AI and to address the new challenges that it brings" (European Commission, 2018a), the Commission calls for a joint effort of the member states to ensure that Europe remains competitive in the global market for AI applications, that no one is left behind in the digital transformation, and that AI technologies are based on values and fundamental rights and therefore can be trusted. Through these objectives, the Commission not only aligns its policy goals with its vision of a 'human-centric AI' but also re-imagines the EU as a political space that provides for the well-being of its citizens and the protection of their fundamental rights. This version of the European Project is particularly important in the face of Europe's current crisis of legitimacy which is not least a crisis of trust (Wilde, 2021). In the early phases of European integration, citizens' trust was primarily connected to the promise of keeping peace and stability on the continent. Today, public trust in the institutions of the EU is, among other factors, challenged by the ongoing digitalization of European societies and its present or possible future impact on the living conditions of Europe's citizens (Bakardjieva Engelbrekt et al., 2019). As many surveys show, privacy intrusions made possible by the extensive use of digital technologies and digital data gathering have led to an erosion of trust which can hit both public and private actors (Wright, 2020). For instance, a survey of 27.000 Europeans found that 59% of those surveyed do not trust their governments who might be regularly capturing large amounts of data on citizens for surveillance purposes (Friedewald et al., 2017). The commitment to developing "trustworthy AI" (European Commission, 2018b: 4), hence, can be understood as a reaction to the EU's 'crisis of trust' by issuing a mission statement that is to re-strengthen citizen's trust in technoscientific progress and the political institutions that aim to govern it.

This mission, however, goes beyond the EU as the Commission puts the Union in a global pioneering role: "The EU can lead the way in developing and using AI for good and for all, building on its values and its strengths." (European Commission, 2018a). The ambition to become the "world-leading region for developing and deploying cutting-edge, ethical and secure AI" (European Commission, 2018c: 1) is framed as a matter of global responsibility. Thereby, its approach to AI is presented as a third way between the unrestrained, market-driven way of the U.S., where (big) tech companies play the central role in R&D and the lack of privacy regulations and data protection enables extensive (consumer) surveillance, and the way of China, where a strong state is the driving force of a coordinated R&D with the overall goal to maintain social harmony and to enable behaviour control. Given the market dominance and expansive strategies of big U.S. tech companies on the one hand and China's endeavour to gain global leadership by means of technology policy, on the other hand, dependency in the AI sector means dependency on actors whose approaches to govern the disruptive potentials and shape the future of AI would differ significantly from the one of the EU. Against the backdrop of the threat scenarios of an AI-powered surveillance capitalism and an AI-powered surveillance state, public trust *in* and acceptance *of* AI is seen as a long-term competitive advantage for the European economy, since they are a prerequisite for the uptake and embedding of AI in society. Achieving a competitive edge through trust, however, would require to effectively manage the risks of AI, "for example in the areas of safety and liability, security (criminal use or attacks), bias and discrimination." (European Commission, 2018a). In the face of these risks, the Commission sets out the essential components of a 'European approach to AI' that not only fosters innovation but also consolidates ethical and legal regulation.

The innovation pillar of this approach aims to "boost the EU's technological and industrial capacity and AI uptake across the economy" (European Commission, 2018a). Given its strategic importance for the competitiveness of the European economy, the EU's ability to deal with societal grand challenges and the aim to regain trust in its institutions, AI has been classified as one of the critical technology areas in which the European Commission strives to achieve 'technological sovereignty' which president Ursula von der Leyen defines as "the capability that Europe must have to make its own choices, based on its own values, respecting its own rules" (von der Leyen, 2019). This essentially means that the EU should not be dependent on AI-based products and services produced *in* or provided *by* companies outside the EU – particularly those from the U.S. and China.

The regulatory pillar of the 'European approach to AI' aims to create an "appropriate ethical and legal framework" (European Commission, 2018a) in line with the Charter of Fundamental Rights and the five ethical principles defined by the European Group on Ethics in Science and New Technologies (European Commission et al., 2018), namely: human dignity, autonomy, responsibility, data protection/privacy, and sustainability. Concerning ethics, the Commission's AI strategy refers to existing normative concepts, such as *explainable AI* and *responsible AI*. The task of developing a solid ethical framework, however, has been delegated to an independent High-Level Expert Group on Artificial Intelligence (AI HLEG).

The AI HLEG presented its ethics guidelines in April 2019, stating that a *trustworthy AI* is lawful, ethical and robust. The AI HLEG states that both technical and non-technical methods can be used for achieving the trustworthiness of an AI application and describes a variety of these non-technical methods such as codes of conduct, standardization, certification and stakeholder participation (High-level Group on Artificial Intelligence, 2019: 22–23). The European Commission, however, highlights technical methods as key principles of their approach to a trustworthy AI and particularly elaborates on so-called 'ethics by design' (European Commission, 2018c: 8). In the terminology of the Commission and the AI HLEG, *ethics by design* stands as an extension of *privacy-by-design* and refers to the implementation of ethical and legal principles since the beginning of the design process. Understood as a method, 'ethics by design' helps to realize the ethically and legally compliant development of AI-based systems by creating "precise and explicit links between the abstract principles which the system is required to respect and the specific implementation decisions" (High-level Group on Artificial Intelligence, 2019: 21). In this rationale, 'ethics by design' constitutes a central feature of a trustworthy AI. If institutionalized ethics is to be understood as a soft regulatory tool for the governance of technology-induced risks (Tallacchini, 2009), the design-in of anticipated ethical implications is to be seen as the subsequent technological hardening of this soft tool.

An essential part of the regulatory pillar, however, remains 'hard' law. In the white paper *On Artificial Intelligence - A European approach to excellence and trust* (European Commission, 2020) and the *Proposal for a Regulation laying down harmonised rules on artificial intelligence* (European Commission, 2021) the European Commission elaborates on mandatory legal requirements that take into account the key requirements of a trustworthy AI as set out by the AI HLEG. Together with the ethical guidelines, these legal requirements constitute the regulatory framework for AI. Besides the main objective to promote trust among citizens, the framework is expected to facilitate the formation of a single market for AI applications and, thus, strengthen the competitiveness of Europe's industry, since the investment *in* and market uptake *of* AI requires legal certainty. Divergent national legislations, on the contrary, are likely to create market fragmentation and obstacles for European companies. Thus, the framework first and foremost has to ensure that „AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values", but at the same time it should not „unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market" (European Commission, 2021: 3). To guarantee this proportionality, the framework sets out a risk-based approach that differentiates between those AI applications that are to be classified as an unacceptable risk, high risk, and low or minimal risk. The mandatory legal requirements only legally apply to those AI applications classified as high risk. In these cases, a conformity assessment and certification process are necessary before an AI application can be put on the market. For low or minimal risk applications only voluntary codes of conduct are envisioned. Certain AI practices, however, are prohibited as "contravening Union values" (European Commission, 2021: 3), for instance, if they are used to manipulate persons through subliminal techniques, for general social scoring and for video surveillance of public spaces. For the latter, however, certain types of criminal investigations where the public interest outweighs the risks are defined as exceptions (European Commission, 2021: 43–44). Moreover, it is stated that the regulation does not apply to AI systems "developed or used exclusively for military purposes" (European Commission, 2021: 39). This reserve takes into account the ongoing controversy between those EU members who are advocating for inaction and those who willing to ban LAWS (Barbé and Badell, 2020). In terms of addressing the high-risks of AI, the EU's regulatory approach clearly enacts the global ambitions of the EU. On the one hand, it implicitly addresses the criticisms of China's notorious Social Scoring System and invasive sales strategies of big U.S. tech companies by classifying these practices as "unacceptable". On the other hand, it defines exceptions *from* and applicability *of* legal constraints in such a way that leveraging

AI for civil security and defence measures will still be possible.

The articulation of the vision of a "human-centric AI" and the measures that have been put in place according to this vision are to be seen as a form of acceptance politics (Barben, 2010) since the EU's regulatory framework is supposed to build up trust and, thus, provide the foundation for the uptake of AI in society: while ethical expert groups would produce trustworthy policy recommendations and engineers would use ethics by design methods to develop trustworthy technology, institutionalized risk assessment, mandatory legal requirements for high-risk applications, and the prohibition of certain, 'unacceptable' AI practices would ensure that EU citizens will have to deal with trustworthy AI only. In economic terms, the 'European approach to AI' is a unique selling position that serves the competitiveness of Europe's economy and helps to fulfil the EU's ambition to become a global player in AI. The purpose of this approach, however, goes beyond legitimizing the complementarity of innovation and regulation, of economics and ethics. Against the backdrop of a diverse spectrum of AI-related fears and AI-related promises, the endeavour to promote public trust in AI becomes deeply intertwined with the endeavour to restore trust in the EU in times of its crisis.

Conclusion

It has been shown how technological expectations have been influential in the creation of European institutions, R&D programmes and regulatory instruments and how they have contributed to processes of European integration. By drawing attention to these links between the formation of a European government and politics on the one side and the problems certain technologies pose and the potential benefits they promise on the other side, the paper addresses the making of Europe as a 'multiply imagined community' (Jasanoff, 2005: 10) based on various technoscientific promises: The promise of nuclear energy was used to promote the creation of a supranational union that would provide for everlasting economic growth and security in its member states. The promise of 'technosecurity' has shaped the EU's joint R&D programme according to the vision of a 'Security Union' where the actors involved agree on a shared responsibility for protecting European citizens in compliance with their fundamental rights. And the vision of a 'human-centric AI' is mobilized to re-imagine the EU as a political space that provides for the well-being of its citizens and the protection of their fundamental rights.

Throughout these processes of re-imaging the European project, however, a few recurrent themes for a European government and politics emerged. One of them is the problem of constructing a single market. The pairing of the two European Communities – EURATOM and the EEC – highlighted the joint endeavour in nuclear energy as a necessary complementary approach to the project of a common market. Funding for cross-border collaboration under the ESPR is expected to break down the fragmentation across Europe's security sector and create a single market for security products. The EU's regulatory framework is expected to facilitate the formation of a single market for AI applications since the investment *in* and market uptake *of* AI requires legal certainty.

Another recurrent theme is the security-technology-nexus. The development of a nuclear industry was considered to be of strategic value with regard to energy security and thus imperative to sustain economic growth and political stability on the continent. The development of advanced technologies and tools is considered to be an adequate solution to deal with a heterogeneous spectrum of security threats and, hence, became the main objective of the EU's security research. The development of trustworthy AI applications is considered to serve the aim of mitigating the risks posed both by an AI-based surveillance capitalism and an AI-based surveillance state.

Furthermore, boundary work to navigate between the civil and the military use of technologies is pervasive. In the case of nuclear power, an artificial distinction is established between the promises and the fears associated with the technology. Consequently, engagement with Big Science cooperation is exclusively connected to nuclear energy whereas the option of developing a common nuclear bomb was never seriously considered. Boundary work is also salient in

EURATOM's system of nuclear safeguards that were installed to ensure that civil nuclear material is not diverted for military purposes. In the case of security technologies, the threats they are expected to protect against blur the boundary between civil and military security. This is reflected within European security research by promoting dual-use R&D despite the declared exclusive civil nature of funding. In the case of AI, the combination of innovation and ethics would ensure that AI is only used for the common good. Therefore, the use of LAWs is addressed on the level of soft law but excluded from the regulatory proposal of the European Commission in order to avoid establishing strict boundaries for future applications.

The paper has covered wide historical ground and uncovered general connections. Such an exercise has its limits in terms of its level of detail and differentiation. But it can nonetheless be of value for both technology-oriented histories and 'standard' political histories of European integration.

Acknowledgements

I am grateful to the anonymous reviewers and to the editor for their extensive feedback and helpful suggestions. This research was supported by Fritz Thyssen Foundation (AZ 10.20.1.015SO).

References

Aas KF, Gundhus HO and Lomell HM (eds) (2009) *Technologies of inSecurity: The surveillance of everyday life*. Abingdon England: Routledge-Cavendish.

Armand L (1955) *Some Aspects of the European Energy Problem: Suggestions for Collective Action.* Report prepared for the Organisation for European Co-Operation, June 1955.

Armand L, Etzel F and Giordani F (1957) *A Target for EURATOM*. Report to the governments of the six Member States of the European Coal and Steel Community, May 1957.

Bakardjieva Engelbrekt A, Bremberg N, Michalski A and Oxelheim L(2019) Trust in the European Union: What Is It and How Does It Matter? In: Bakardjieva Engelbrekt A, Bremberg N, Michalski A and Oxelheim L (eds) *Trust in the European Union in Challenging Times:*.Cham: Springer International Publishing, pp. 1–22.

Barbé E and Badell D (2020) The European Union and Lethal Autonomous Weapons Systems: United in Diversity? In: Johansson-Nogués E, Vlaskamp MC and Barbé E (eds) *European Union Contested.* Cham: Springer International Publishing, pp. 133–152.

Barben D (2010) Analyzing acceptance politics: Towards an epistemological shift in the public understanding of science and technology. *Public Understanding of Science* 19(3): 274–292.

Barry A (2001) *Political machines: Governing a technological society*. London: Athlone Press.

Barry A and Walters W (2003) From EURATOM to "Complex Systems": Technology and European Government. *Alternatives: Global, Local, Political* 28(3): 305–329.

Beck U (1998) *World risk society*. Cambridge, Massachusetts: Polity Press.

Beckert J (2013) Imagined futures: Fictional expectations in the economy. *Theory and Society* 42(3): 219–240.

Bigo D and Carrera S (2005) From New York to Madrid: technology as the ultra-solution to the permanent state of fear and emergency in the EU. *CEPS Commentary*, CEPS, Brussels, April.

Bigo D and Jaendeboz J (2010) The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. *IN: EX Policy Brief* (5).

Boin A, Ekengren M and Rhinard M (2006) Protecting the Union: Analysing an Emerging Policy Space. *Journal of European Integration* 28(5): 405–421.

Brown N, Rappert B and Webster A (eds) (2000) *Contested futures: A sociology of prospective techno-science*. London, New York: Routledge Taylor & Francis Group.

Ceyhan A (2008) Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance and Society* 5(2): 102–123.

Citi M (2014) Revisiting Creeping Competences in the EU: The Case of Security R&D Policy. *Journal of European Integration* 36(2): 135–151.

Comité intergouvernemental créé par la conférence de Messine (1956) *Rapport des chefs de délégation aux ministres des affaires etrangères*. Spaak report, April 1956.

Commission of the European Communities (1955) *The Messina Declaration*. Available at: https://www.cvce.eu/obj/resolution_adopted_by_the_foreign_ministers_of_the_ecsc_member_states_messina_1_to_3_june_1955-en-d1086bae-0c13-4a00-8608-73c75ce54fad.html (accessed 28 October 2022).

Commission of the European Communities (1968) *Survey of the nuclear policy of the European Community*. Report to the Council of the European Union, Octobre 1968.

Council of the European Union (2010) *Draft Internal Security Strategy for the European Union: Towards a European Security Model*. March 2010.

Cramer KC (2020) *A Political History of Big Science*. Cham: Springer International Publishing.

Cronqvist M, Farbøl R and Sylvest C (2022) *Cold War Civil Defence in Western Europe*. Cham: Springer International Publishing.

Dillon M (2002) Network Society, Network-centric Warfare and the State of Emergency. *Theory, Culture & Society* 19(4): 71–79.

Egeland K and Pelopidas B (2021) European nuclear weapons? Zombie debates and nuclear realities. *European Security* 30(2): 237–258.

EURATOM (1958) *Treaty establishing the European Atomic Energy Community*.

European Atomic Energy Society (1954) *Nature* 174(4423): 251–252.

European Commission (2004) *Research for a Secure Europe*. Report of the Group of Personalities in the field of Security Research, March 2004.

European Commission (2012) *Security Industrial Policy: Action Plan for an innovative and competitive Security Industry*. Communication to the European Parliament, the Council and the European Economic and Social Committee, July 2012.

European Commission (2013) *HORIZON 2020. Work Programme 2014 – 2015. 14. Secure societies – Protecting freedom and security of Europe and its citizens.* Decembre 2013.

European Commission (2014) *Ethics of security and surveillance technologies: Opinion No. 28 of the European Group on Ethics in Science and New Technologies*.

European Commission (2015) *The European Agenda on Security*. Communication to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions, April 2015.

European Commission (2016a) *Delivering on the European Agenda on Security to fight against terrorism and pave the the way towards an effective and genuine Security Union*. Communication to the European Parliament, the European Council and the Council, April 2016.

European Commission (2016b) *Security Research: Future-bound to protect our society*. August 2016.

European Commission (2017) *LAB – FAB – APP: Investing in the European future we want*. Report of the independent High Level Group on maximising the impact of EU Research & Innovation Programmes, July 2017.

European Commission (2018a) *Artificial Intelligence for Europe*. Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, April 2018.

European Commission (2018b) *Coordinated Plan on Artificial Intelligence*. Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Decembre 2018.

European Commission (2018c) *Coordinated Plan on Artificial Intelligence: Annex*. Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Decembre 2018.

European Commission (2018d) *From Research to Security Union*. March 2018.

European Commission (2020) *White Paper on Artificial Intelligence: A European approach to excellence and trust*. February 2020.

European Commission (2021) *Proposal for a Regulation laying down harmonised rules on artificial intelligence*. April 2021.

European Commission and Directorate-General for Research and Innovation (2007) *Taking European knowledge society seriously*. Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission, January 2007.

European Commission, Directorate-General for Research and Innovation and European Group on Ethics in Science and New Technologies (2018) *Statement on artificial intelligence, robotics and 'autonomous' systems Brussels, 9 March 2018*. Publications Office.

European Council (2010) *Stockholm Programme: An open and secure Europe serving and protecting citizens*. May 2010.

European Parliament (2002) *The European Parliament and the Euratom Treaty: past, present and future*. Decembre 2001.

European Parliament (2017) *Report with recommendations to the Commission on Civil Law Rules on Robotics*. January 2017.

European Security Research and Innovation Forum (2009) *ESRIF Final Report*. Decembre 2009

European Union (1997) Treaty of Amsterdam Amending the Treaty on European Union, The Treaties Establishing the European Communities and Related Acts. Available at: https://eur-lex.europa.eu/eli/treaty/ams/sign (accessed 28 October 2022).

European Union (2007) Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. Available at: https://eur-lex.europa.eu/eli/treaty/lis/sign (accessed 28 October 2022).

Friedewald M, Burgess JP, *Čas* J, Bellanova R and Peissl W (2017) *Surveillance, Privacy and Security*. New York: Routledge.

Fujimura J (2003) Future imaginaries: genome scientists as sociocultural entrepreneurs. In: Goodman AH, Heath D and Lindee MSL (eds) *Genetic nature/culture: Anthropology and science beyond the two-culture divide*. Berkeley: University of California Press, pp. 176–195.

Hälterlein J (2021) Epistemologies of predictive policing: Mathematical social science, social physics and machine learning. *Big Data & Society* 8(1): 205395172110031.

Hälterlein J, Madsen L, Schuchardt A, Peperhove R and Gerhold L (2018) Integrating Volunteers in Emergency Response: A Strategy for Increased Resilience Within German Civil Security Research. In: Fekete A and Fiedrich F (eds) *Urban Disaster Resilience and Security: Addressing Risks in Societies*. Basel: Springer International Publishing, pp. 113–128.

Hecht G (1998) *The radiance of France: Nuclear power and national identity after World War II*. Cambridge, Mass: MIT Press.

Hecht G (2006) Nuclear Ontologies. *Constellations* 13(3): 320–331.

High-level Group on Artificial Intelligence (2019) *Ethics Guidelines for trustworthy AI*. April 2019.

Hilgartner S, Prainsack B and Hurlbut JB (2017) Ethics as Governance in Genomics and Beyond. In: Felt U, Fouché R, Miller CA and Smith-Doerr L (eds) *The handbook of science and technology studies.* Cambridge, Massachusetts, London, England: The MIT Press, pp. 823–851.

Holloway D (1994) *Stalin and the bomb: The Soviet Union and atomic energy, 1939 - 1956*. New Haven: Yale Univ. Press.

Jasanoff S (2005) *Designs on Nature: Science and Democracy in Europe and the United States*. Princeton: Princeton University Press.

Jasanoff S and Kim S-H (2009) Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea. *Minerva* 47(2): 119–146.

Kaijser A (2021) *Engaging the Atom: The History of Nuclear Energy and Society in Europe from the 1950s to the Present*. Morgantown: West Virginia University Press.

Konrad K, van Lente H, Groves CJ and Selin C (2017) Performing and Governing the Future in Science and Technology. In: Felt U, Fouché R, Miller CA and Smith-Doerr L (eds) *The handbook of science and technology studies.* Cambridge, Massachusetts, London, England: The MIT Press, pp. 465–493.

Krige J (2006) Atoms for Peace, Scientific Internationalism, and Scientific Intelligence. *Osiris* 21(1): 161–181.

Krige J (2008) The Peaceful Atom as Political Weapon: Euratom and American Foreign Policy in the Late 1950s. *Historical Studies in the Natural Sciences* 38(1): 5–44.

Krige J (2016) *Sharing knowledge, shaping Europe: U.S. technological collaboration and nonproliferation*. Cambridge, MA, London: The MIT Press.

Lakoff A and Collier SJ (2010) Infrastructure and Event: The Political Technology of Preparedness. In: Braun B and Whatmore S (eds) *Political matter: Technoscience, democracy, and public life*. Minneapolis: University of Minnesota Press, pp. 243–266.

Lalli R (2021) Crafting Europe from CERN to Dubna: Physics as diplomacy in the foundation of the European Physical Society. *Centaurus* 63(1): 103–131.

Leese M (2015) 'We were taken by surprise': Body Scanners, Technology Adjustment, and the Eradication of Failure. *Critical Studies on Security* 3: 269–282.

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

Mager A (2017) Search engine imaginary: Visions and values in the co-production of search technology and Europe. *Social Studies of Science* 47(2): 240–262.

Marx GT (2001) Technology and social control: The search for the illusive silver bullet. In: Smelser NJ and Baltes PB (eds) *International encyclopedia of the social & behavioral sciences.* Amsterdam, Boston, Heidelberg, London: Elsevier, pp. 15506–15512.

Mattelart A (2010) *The Globalization of Surveillance*. Hoboken, NJ: Wiley.

Minsky M (1986) *The society of mind*. New York: Simon and Schuster.

Misa TJ and Schot J (2005) Introduction. *History and Technology* 21(1): 1–19.

Mobach K and Felt U (2022) On the Entanglement of Science and Europe at CERN: The Temporal Dynamics of a Coproductive Relationship. *Science as Culture*: 1–26.

Möllers N and Hälterlein J (2013) Privacy issues in public discourse: the case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research* 26(1-2): 57–70.

Moravec H (1995) *Mind children: The future of robot and human intelligence*. Cambridge: Harvard University Press.

Nieburg HL (1963) EURATOM: A Study in Coalition Politics. *World Politics* 15(4): 597–622.

Pavone V and Degli Esposti S (2012) Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science* 21(5): 556–572.

Rhodes R (1988) *The making of the atomic bomb*. London: Penguin Books.

Richers J, Lüscher F and Guth S (2018) Nuclear Technopolitics in the Soviet Union and Beyond – An Introduction. *Jahrbücher für Geschichte Osteuropas* 66(1): 3.

Sagan SD (1996) Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb. *International Security* 21(3): 54.

Sauer T (2020) Power and Nuclear Weapons: The Case of the European Union. *Journal for Peace and Nuclear Disarmament* 3(1): 41–59.

Sovacool BK (2011) *Contesting the Future of Nuclear Power*. Singapore: WORLD SCIENTIFIC.

Spiering M (2011) Atoms for Europe. In: Spiering M and Wintle M (eds) *European identity and the Second World War*. Basingstoke: Palgrave Macmillan, pp. 171–185.

Tallacchini M (2009) Governing by Values. EU Ethics: Soft Tool, Hard Effects. *Minerva* 47(3): 281–306.

Trischler H and Bud R (2018) Public technology: nuclear energy in Europe. *History and Technology* 34(3-4): 187–212.

van der Vleuten E, Högselius P, Hommels A and Kaijser A (2013) Europe's Critical Infrastructure and its Vulnerabilities: Promises, Problems, Paradoxes. In: Högselius P, Hommels A, Kaijser A and van der Vleuten E (eds) *The Making of Europe's Critical Infrastructure: Common Connections and Shared Vulnerabilities*. Basingstoke: Palgrave Macmillan, pp. 3–19.

von der Leyen U (2019) *A Union that strives for more: My agenda for Europe*. Political Guidelines for the next European Commission 2019-2024. Octobre 2019.

Weart SR (2012) *The rise of nuclear fear*. Cambridge, Mass: Harvard University Press.

Weizenbaum J (1976) *Computer power and human reason*. San Francisco: Freeman.

Welsh I (2000) *Mobilising modernity: The nuclear moment*. London and New York: Routledge.

Wilde P de (2021) Rebound? The Short- and Long-Term Effects of Crises on Public Support and Trust in European Governance. In: Riddervold M, Trondal J and Newsome A (eds) *The Palgrave Handbook of EU Crises*. Cham: Springer International Publishing, pp. 667–683.

Winner L (2004) Trust and terror: the vulnerability of complex socio-technical systems. *Science as Culture* 13(2): 155–172.

Wolf S (2011) Euratom Before the Court: A Political Theory of Legal Non-Integration. *European Integration Online Papers* 15(10).

Wright D (2020) Privacy and trust at risk in surveillance societies. In: European Commission (ed) *Trust at Risk: Implications for EU Policies and Institutions*. Report of the Expert Group "Trust at Risk? Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT). Luxembourg, pp. 48–68.

Notes

1 See for instance the Tensions of Europe Research Network; https://www.tensionsofeurope.eu/

2 In 1957, the French government approached Germany and Italy with the proposal for a joint development and production of nuclear weapons, resulting in a trilateral agreement in 1958. However, the endeavour ground to a halt following the rise to power of Charles de Gaulle later in 1958, who strongly opposed German access to nuclear weapons (Egeland and Pelopidas, 2021).

3 An alternative for transnational collaboration in the field of nuclear energy was established with the European Nuclear Energy Agency (ENEA), organized under the auspices of the OEEC and formally established in December 1957. The ENEA was a more loosely structured institutional framework and should not involve the pooling of resources nor should it restrict the national sovereignty of its members in any way. (Nieburg, 1963: 597).

4 The U.K., on the contrary, after having participated in the preparatory phase of the treaty negotiations, decided to step back and to work through the OEEC in which it played a leading role.

5 Both groups comprised EU commissioners, selected security scholars, national defence ministers from member states and the CEOs of most of the largest European security industry corporations.

6 For a detailed analysis and critique of the ethics review process within the ESRP see: (Leese et al., 2019: 63–66).