Chapter 7

Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies

János Székely

Abstract

This chapter aims to address the problem presented by governance regimes applicable to the dual (civilian and military) use of emerging and disruptive technologies such as artificial intelligence and biotechnology. The author first examines the definition of "dual use" as it emerges from various unilateral and multilateral governance instruments. As several definitions currently coexist, "dual use" is found to constitute a fuzzy notion, requiring clarification in further regulation and application. The major regimes governing dual-use technology proliferation and trade are presented with an emphasis on the role of securitisation in determining the applied regulatory approach and content. The technological and economic rivalry between the United States of America and the People's Republic of China was found to have a defining role in the current transformation of such governance regimes to the detriment of free trade. Subsequently, the problems posed by artificial intelligence, biotechnology, and 5G broadband data transfer were examined in light of dual-use technology regulation, with conclusions presented regarding the future desirable development of the regulatory environment.

Keywords: dual-use, emerging technology, disruptive technology, securitisation, export control.

János Székely (2024) 'Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 309–353. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_7

1. Introduction

1.1. Dual use as a result of technological synergies

Technological and scientific development and warfare are closely associated. Some of the defining inventions of modern life itself, in fields ranging from power generation to medicine, manufacturing to telecommunications, and transportation to data processing, have either been employed during warfare or, quite often, have even been developed[1] specifically with warfare in mind. Thus, some technologies have peaceful and war-like applications simultaneously while requiring little to no adaptation to suit either purpose. These are the situations to which the notion of dual-use technology, in its broadest sense, refers.

The ongoing wars in Ukraine or the Middle East allow us to observe, for example, the deployment[2] of small, toy-like unmanned aerial vehicles ("drones" in common parlance, sometimes abbreviated as UAS in the case of light-weight systems, although henceforth we will refer to them as UAVs) during combat operations.[3] Many of these platforms, unlike larger, military-grade UAVs, were initially designed for hobbyists interested in amateur aerial photography rather than for military use. Adding simple mounts for ammunition to be released over the heads of enemy forces converts what was once conceived of as little more than high-end toys, into weapons of war.

In cases when such dual use occurs, a synergy of different technologies, building on various specialised items and knowledge, is indispensable: to construct an improvised combat UAV, an off-the-shelf product must be modified and reprogrammed by capable personnel. It would not function without advanced telecommunication support (possibly access to the Internet, or some other way of conveying commands and transmitting flight telemetry, as well as image data, likely also requiring electronic countermeasures to evade hostile jamming efforts), access to a global navigation system, or the microprocessors, cameras, remote controllers, screens, antennas, motors, and actuators assembled as a "package" (albeit with a purpose other than war), which permit effective use of the toy-turned-weapon in combat by the operator.

This case is instructive in several respects: First, it demonstrates that technologies thought of as generic or civilian are often of dual use. Second, it shows that the regulation of such technologies, especially by rules intended to prevent their proliferation or hostile use, is difficult to accomplish and may affect free trade and civilian technological development. Third, it shows that whenever we consider dual-use "technologies" in the strict sense, we cannot ignore the categories from which such dual use stems, simply because the technology itself is a result of a synergy

1 Brunk and Jason, 1981, pp. 437–455.
2 Puranik, 2021, pp. 33–52.
3 Thompson, 2024.

(a self-enforcing interaction) between *specialised knowledge* (such as that gained by research and experimentation) and *artefacts*, or *items* (ranging from raw materials, to manufactured – corporeal – goods).[4] Therefore, dual-use knowledge, items, and technologies should all be considered as separate objects of regulation. I shall nonetheless examine them together, as references to dual-use technology oftentimes include not just "technology" in the proper sense of the word, but also knowledge, and items (components) utilised in its makeup.

1.2. The "grey zone" of dual-use technologies

Some knowledge, items, and technologies, such as those whose purpose is evidently the construction of weapons of mass destruction (WMDs), weapon systems, or other possibly destructive end uses (e.g. the aptitudes of some nuclear scientists, rockets and jet engines, highly enriched or weapons-grade fissile materials, reactor containment vessels, precursor chemicals, pathogens, avionics equipment, advanced aerospace alloys, radars and targeting systems, directed energy systems, specialised machine tools, etc.) present obvious dangers, and their identification and strict regulation poses less of a challenge. These fall into a "black zone" of knowledge, items, and technologies (mostly dealt with by non-proliferation conventions and weapons embargos) with clearly defined edges or limits for some obviously destructive purpose.

The difficult question for experts, regulators, and industry alike is how to define and regulate items, technologies, and knowledge that do not fall neatly into this category, but are part of a "grey zone", being (mostly) employed in the civilian sector, or with only marginal obvious significance for warfare, unless some destructive synergies are created, such as the ones which gave rise to the improvised combat UAV. Clearly, weapon systems cannot be reasonably considered as having a "dual use": their single envisaged use is combat itself. Therefore, these will not form the object of my analysis, as they are mainly subject to rules on *stricto sensu* arms control.

Thus, the subject matter of my study shall be constituted by the "grey zone" items, technologies, and knowledge, the proliferation of which, even for civilian use, may result in nefarious applications. This is because this "grey zone" is the one that also includes many of the most significant technological developments for civilian use, and which presents grave implications for global economic interconnectedness, including technological interdependency.

While underregulating dual-use technologies poses significant risks, overregulation or abusive enforcement of regulation may also result in costs, which may have a chilling effect on the development of certain technologies, as during the allocation of funding, such extant or future limitations on their potential markets will be considered. Various regimes regarding dual-use technologies seek mainly to balance national security and national interest concerns with those of business: a high regard

4 For this categorisation, see: Forge, 2010, pp. 112–115.

for national security may be paired with a low or high regard for national business interests, and consideration may also be granted to national business interests as part of national security concerns.[5]

One other problem for national security, which is rarely voiced, but should not be ignored when studying the problems posed by dual-use technology regulation, is the "conversion" of dual-use knowledge, items, and technologies,[6] which permits some flexibility in the transfer of resources between enterprises with a focus on defence or on civilian implementation as desirable. In this manner, defence spending during low-threat periods may be reduced without losing the capability to re-employ resources for defence if needed.[7] Such conversion has the added benefit of camouflaging defence spending, as exemplified by the development of UAV technology using European Union (EU) research funding (e.g. Horizon 2020 projects), through consortia with a hybrid (state and private) structure and also a hybrid (both civilian and military) purpose, which constitute a nascent "European Industrial Military Complex" as a response to recent changes in the strategic environment and the defence needs of EU member states.[8]

1.3. Securitisation as the common element of current dual-use technology regulation

In the field of dual-use technologies, various regulatory regimes aim to address two problems. The difficulties of this endeavour are usually summed up by the 'dual-use dilemma' and the 'dual-use security dilemma'.[9] The former refers to the risk of intentional or accidental misuse (including unintended military use) of knowledge, items, or technology in general and is mainly treated in ethical codes, as well as domestic and international regulatory regimes which aim to prevent misuse. The latter constitutes a behavioural pattern between two actors, where the second fears that the first will develop or acquire dual-use knowledge, items, or technologies to utilise them for military purposes, and aims to prevent such an acquisition. In this second dilemma, every measure one actor takes is considered to have an offensive purpose by the other, leading to a spiral of ever-stricter responses and counter-responses with potentially devastating effects on regional and global trade as well as technological development.

The regulation of dual-use knowledge, items, and technologies may, even without any hostile relations between economic actors, constitute a pretext for erecting tariff-like barriers, thus excluding some actors from markets and resulting in trade policies instituted to create a civilian industrial base, which can then be turned to

5 Seyoum, 2017, pp. 695 et seq.
6 Brandt, 1994, pp. 365 et seq.
7 See: Skolnikoff, 2008, pp. 42–47.
8 Martins and Küsters, 2019, pp. 280 et seq.
9 Lupovici, 2021, pp. 260–263.

war-like purposes.[10] Such policies may also be weaponised as a tool for trade wars aimed at the economic and political containment of not just real adversaries but also economic competitors.

Numerous theories have been proposed to explain the effects of dual-use technology regulations on trade. They recognise the economic impact of such regimes and that they may be implemented solely for their economic effects, including restrictions on free trade.[11] Markets, especially those in the economic spheres of influence of great powers, may be nudged, or outright coerced to only obtain technology from some suppliers, while competition from entities deemed to be "hostile" may be severely restricted. Such theories, widely referred to as economic securitisation, imply that by designating a given domain as being of existential importance within a political unit (i.e. a state or an alliance system) and viewed from the perspective of the common values of that political system, such a domain may be brought under a regulatory regime specific to urgent threats: it may be regulated by means and methods specific to extraordinary rather than ordinary legislation.[12] In simple terms, economic securitisation means that states or alliance systems consider competition from other states or alliance systems with different values or different geopolitical interests as a hostile act, or at the very least as a long-term threat in and of itself, which must be countered by regulatory means specific to (armed) conflicts. These means may include restrictions on trade and technology transfer as well as other measures to stunt the development of the perceived adversary.

The securitisation of dual-use knowledge, items, and technology poses several problems. The primary issue, which must be considered pivotal to future regulation, is whether, by implementing extraordinary measures, the political entity in which this phenomenon occurs (e.g. Western democracies) creates a counterproductive environment for its own economic development, resulting in the re-establishment of isolated geopolitical blocks to the detriment of interconnectivity. Securitisation, in its extreme manifestation, may even result in the fragmentation of scientific progress, especially when, as proposed,[13] even institutions of higher education should observe measures to prevent the undesired transfer of dual-use knowledge, items, and technologies. Tailoring free-trade regimes set forth in various agreements to curtail dual-use technology transfer outside a given alliance structure is also an increasing practice.[14] All these considerations must be addressed concurrently to understand the impact of dual-use technology regimes in the military, civilian, and specifically, the economic and trade fields.

Owing to such considerations, defining the conceptual limits of dual use and the scope of regimes that impose limits on dual-use knowledge, items, and technologies

10 See: Blanken and Lepore, 2024, pp. 192–205.
11 Fuhrmann, 2008, pp. 645–649.
12 Buzan and Wæver, 2009, p. 265. For further details on securitisation theory, see: Taureck, 2006; Floyd, 2007; Stritzel, 2007.
13 See: Gearon, 2017; Gearon and Parsons, 2019.
14 Klaus, 2003, pp. 120–129.

is indispensable. Yet, partly due to the diversity of such regimes, manifested both in sources of soft law, such as scientific ethics codes, and hard domestic and international law instruments, such as acts of legislation or international conventions, and partly due to the diversity of meanings in which "dual use" is utilised, such a definition is elusive.

The fields in which the dual-use problem has arisen are growing in number as various disruptive technologies (such as biotechnology, artificial intelligence, and quantum computing) have emerged from the synergy of new scientific knowledge, novel materials, and other items as well as previous technologies. Therefore, considering the security and economic implications of restrictions imposed owing to the possible dual use of disruptive new technologies, such limitations must be subject to analysis, which I will undertake in the following sections.

This chapter considers dual-use technology regulation mainly from the perspective of technological development and transfer of technology to avoid over-extending the scope of this enquiry. Due to the breadth of the field of regulation, in a context of ever-increasing securitisation of geoeconomic competition, this study cannot offer a comprehensive view of all the relevant regulatory regimes that may affect dual-use technologies. Therefore, my enquiry is limited mostly to export controls, where the dual-use dilemma is present in the sources of soft law, black letter law, and administrative practices. For this reason, I shall specifically exclude – apart from minor references – from the object of this study the problems of foreign investment screening, which is not specifically regulated by major international instruments, and where the relevant EU regulation[15] has been enacted only relatively recently. This regulation realised only partial harmonisation when creating the EU Investment Screening Mechanism (which focuses specifically on information sharing between the member states, as well as between them and the European Commission, and transparency and non-discrimination), and left the most significant part of setting up and operating domestic investment screening regimes to member states (with the marginal positive effect that some member states that did not operate such screening were induced to create these mechanisms).[16] Consequently, the possible interactions between measures taken to prevent access to dual-use technology by making use of foreign direct investment oversight[17] against potential adversaries and export controls will not be analysed separately.

15 *Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (consolidated text)*, 2019.

16 Bauerle-Danzman and Meunier, 2024, pp. 8–9, 14–15.

17 See: Zwartkruis, 2024.

2. Defining dual use

Defining dual use as referring to knowledge, items, or technologies is fiendishly difficult. Determining the meaning of dual use as an expression constitutes just one layer of the complexity involved. This is because dual-use concepts in sources of hard or soft law, legal (and ethics) literature, and doctrine are by no means unitary; in fact, there exist numerous framings of this notion in both normative instruments and the relevant literature.[18] Some of these conceptually overlap.

Originally, the term "dual use" was clearly meant to achieve the delineation of technologies that may be turned to military or civilian purposes alike, from those (few) which did not pose such risks; this meaning was however superseded with the advent of legal instruments aimed at ensuring non-proliferation of various technologies, especially the prevention of terrorism, through export controls.[19] In this sense, military use was essentially supplanted by malevolent, destructive, or illegal use.[20]

One possible model for the historic transformation of the concept of dual use was charted by Rath et al., who considered national and international non-proliferation and antiterrorism instruments according to the following scheme:

1. dual use in the meaning of a concomitant, i.e. dual civilian, and military purpose for the regulated knowledge, item, or technology complemented by the notions of benevolent or malevolent purpose, when discussing dual use in anti-terrorism, or anti-criminal contexts (with an added distinction between accepted use by allies, and unaccepted use by non-allies) – this concept is present in both national and international, multilateral instruments,
2. dual use, as taken in the above-mentioned civilian–military (or law-enforcement) as well as benevolent–malevolent dichotomies, complemented by a specific meaning of benevolent, or malevolent purpose understood in the context of human rights protection (i.e. the propensity for an end-use of proscribed knowledge, items or technology in order to restrict exercise of, or infringe on human rights) – this concept is mostly present in national (and regional), unilateral instruments,
3. dual use in the meaning of peaceful and non-peaceful purpose of the regulated knowledge, item or technology, a situation encountered in the non-proliferation regimes specifically designed to prevent the spread of weapons of mass destruction (WMDs) – this meaning is usually found in multilateral instruments,
4. dual use in the context of biosecurity oversight, where instead of the traditional dichotomies mentioned above (which consider the – sometimes

18 See: Rath, Ischi and Perkins, 2014; Miller, 2018; Sánchez-Cobaleda, 2022.

19 Rath, Ischi and Perkins, 2014, p. 770.

20 For the possible use categories of technologies deemed as possibly of dual use, including political use for restricting basic freedoms, and the analysis of the difficulties presupposed by defining such categories, see: Mahfoud et al., 2018.

presumed – purpose or use-case), the risks posed by the regulated knowledge or item is considered, especially regarding whether it could be wilfully, or inadvertently diverted from its original purpose, thus giving rise to a risk-based approach, which transcends the known or presumed intentions of the user – this approach is specific to ethics guidelines in scientific research.[21]

Regarding the presence of the notion of dual use in various major international instruments, it has been shown[22] that the Treaty on the Non-Proliferation of Nuclear Weapons[23] only refers to dual use indirectly (when mentioning fissile – "fissionable" – materials); the Biological Weapons Convention[24] refers to the purpose of use of certain biological agents, an approach that is mirrored by the Chemical Weapons Convention[25] (however, the latter also includes schedules listing substances that are to be considered as being of potential dual use), while UN Security Council Resolution 1540 (2004) employs the notion of dual use materials only implicitly, with reference to proscribed materials lists.[26] Other – mostly non-binding (soft law), even if regularly adhered to – instruments, such as the Nuclear Suppliers Group Guidelines,[27] the Missile Technology Control Regime Guidelines,[28] and the Australia Group Guidelines and Common Control Lists[29] employ the notion of "dual use" explicitly, usually to refer to the substances, items, technology, and software included in specific proscription lists.[30] Among international soft-law instruments, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[31] stands out (as the successor regime to the previous Coordinating Committee for Multilateral Export Controls, or COCOM, arrangement), as its rules attempt to define dual use by separating military and nonmilitary utilisation of the various items to which it refers.[32]

21 Rath, Ischi and Perkins, 2014, pp. 771–779. A situation related to this last meaning of the notion of dual use may also be conceived in the case of artificial intelligence and other disruptive technologies (e.g. nanotechnology, quantum computing, etc.) which by their possibly world-altering effects would only be comparable to biotechnology, but which, due to their theoretical nature, are as of yet unregulated or underregulated.

22 Rath, Ischi and Perkins, 2014, pp. 774–777; Sánchez-Cobaleda, 2022, pp. 77–95.

23 *Treaty on the Non-Proliferation of Nuclear Weapons*, 1968.

24 *The Biological Weapons Convention*, 1972.

25 *Chemical Weapons Convention*, 1993.

26 'Related materials: materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery'. UNODA, 2004.

27 *Nuclear Suppliers Group Guidelines*, no date.

28 *Missile Technology Control Regime Guidelines*, 2023.

29 The Australia Group, no date b.

30 Rath, Ischi and Perkins, 2014, pp. 771–777; Sánchez-Cobaleda, 2022, pp. 77–95.

31 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, 1995.

32 Rath, Ischi and Perkins, 2014, p. 774; Sánchez-Cobaleda, 2022, pp. 77–95.

Thus, the concept of dual use is, apparently, inextricably linked to what have been referred to as 'purpose concepts',[33] in fact, dichotomies of "desirable" and "undesirable" purposes, and which may be summarised as follows: a civilian or a military purpose, a benign (non-destructive) or a malevolent (destructive) purpose, a peaceful or a non-peaceful purpose, a legitimate or an illegitimate purpose (from the perspective of national security and human rights), and finally a "good" military or a "good" civilian purpose, as opposed to "bad" civilian and "bad" military purposes (mostly significant in the case of technologies with important civilian uses).

It should be emphasised here that while the literature recognises the case of dual use, where such use may be inadvertent (i.e. in the form of risk-based ethical regulation), this cannot be comfortably squared with any of the above-mentioned dualist categories, which implicitly assume the existence or possibility of a purpose, that is, are based on the presumed intentions of the user.

This, in turn, renders the concept of dual use vulnerable to misconstruction based on the regulator's intrinsic perspective, instead of on any set of objective criteria. Thus, the risk of dual use may at times just be in the eye of the beholder, that is, it may depend more on irrational elements than on any objective criterion.[34]

This conclusion underscores one of the major issues that I would like to address in this chapter: In the regimes set up to regulate dual-use knowledge, items, and technology, the casuistic approach runs rampant. Such a method of regulation, even of soft-law norms such as ethics codes, is particularly problematic in the case of scientific knowledge already gained and cutting-edge research, where in both life sciences and artificial intelligence, the notion of 'dual-use research of concern'[35] has evolved, just as dual use previously did, very much under the radar of legal scholarship.

The complementary concepts of knowledge, items, and technology are also somewhat problematic, as they may include tangible items or entire technologies (materials, plans, research results, microprocessors, UAVs, etc.) but almost always present an intangible component in the form of education, training, and know-how.[36]

Thus, the conceptual systematisation of rules pertaining to dual-use knowledge, items, and technologies is an evident necessity. In the international arms control law literature, a fourfold system of factors has been developed to determine if an item should be proscribed (including as being dual-use), which may also be readily applied to dual-use technology regulation in its entirety:

> Whether or not an authorization for the export of an item is required will, in general, be determined by answering the "what", "where", "who", and "how" questions. What

33 Rath, Ischi and Perkins, 2014, pp. 779–783; Sánchez-Cobaleda, 2022, pp. 77–95.

34 This phenomenon is present in the 'I'll know it when I'll see it' doctrine developed by the Supreme Court of the United States in the case of *Jacobellis v. Ohio* (1964), when it was used to avoid providing a detailed definition of the concept of "pornography". Gewirtz, 1996, p. 1026; Rath, Ischi and Perkins, 2014, p. 777.

35 Urbina et al., 2022, p. 607.

36 On this problem, see: Katz, 2020; Sánchez-Cobaleda, 2022.

are the product specifications of an item, and do they correspond with a listed item (classification)? Where is an item heading (destination); is that State subject to a sanctions regime? Who is ultimately the user of the item (end-user)? And finally, how will the item ultimately be used (end-use)?[37]

Such a system, when adapted to the regulation of dual-use knowledge, items, and technologies, could be used to summarise and systematise the approaches described above. This tentative systematisation is presented in the following table:

Table 1. Summary of approaches to the various definitions of dual use (author's own).

Context of dual-use definition	Main characteristic of use category	Dual-use character determined according to:	Instruments
Traditional perspective	civilian / military use	end use	national and international (multilateral); binding and non-binding
Positional[38] perspective	use by an ally / use by an adversary	end user, end use	mostly national and regional (e.g. EU) binding instruments
	accepted use / unaccepted use	end use	
Law-enforcement and anti-terrorism perspective	legal use / illegal use	end user, end use	national and international (multilateral), binding and non-binding instruments
Human rights perspective	potential use infringing on human rights	end user, end use	national and regional unilateral instruments

37 Voetelink, 2022, p. 72.

38 What I choose to call a "positional" definition here refers to provisions contingent on the status (position) of an actor. Under such a definition, the very same conduct may be legal when exercised by one actor, and illegal when exercised by another. Such positional rules regularly result from value-system principles (moral, political, and ethical principles) that imbue legal rules with external values (such as states under a rule of law, as opposed to states considered autocracies). These values are sometimes subject to sudden change. See: Kelsen, 1991, p. 115.

Context of dual-use definition	Main characteristic of use category	Dual-use character determined according to:	Instruments
Non-proliferation of WMD perspective	potential nefarious (non-peaceful) use	classification, destination, end user	binding international (multilateral) instruments, national instruments
Biosecurity and life sciences perspective	potential for unethical, risky, or nefarious (non-peaceful) use	classification, end user, end use	non-binding ethics codes

I consider that the concept of dual use as well as all complementary concepts indicated above constitute what is called, including in legal science, a *fuzzy set*, that is, a set whose elements cannot be clearly defined, with some meanings possibly outside the set, as well as inside it, and major conceptual overlaps, depending on subjectively attributed criteria (resulting from the "I'll know it when I'll see it" approach intrinsic to the regulation of the topic).[39] This is a well-known problem in instruments aimed at achieving non-proliferation and arms control, where the use of imprecisely defined notions is both intentional and problematic, not just allowing political manoeuvring, but also inadvertent misunderstanding[40] when it comes to potential dual-use knowledge, items, or technologies subject to the imposed measures.

The creation of a functional normative definition of dual-use technology has also been attempted. In our opinion, the best definition to date was proposed by Forge and is as follows:

> An item (knowledge, technology, artefact) is dual use if there is a (sufficiently high) risk that it can be used to design or produce a weapon, or if there is a (sufficiently great) threat that it can be used in an improvised weapon, where in neither case is weapons development the intended or primary purpose.[41]

The author aptly notes immediately after the definition that 'The judgements about risk and threat are contextual […]. Also, the definition presupposes a system of values that informs the general attitude to weapons production as bad because it provides the means to harm'.[42]

In this way, the subjective complementary content of the definition stands clearly recognised: this definition, and in fact any attempt at a normative definition of dual use, is predicated on first creating a moral framework for acceptable and unacceptable

39 See: Legrand, 1999, p. 238.
40 Bremer-Maerli and Johnston, 2002, pp. 54–56.
41 Forge, 2010, p. 117.
42 Forge, 2010, pp. 117–118.

use that will inherently constitute a value-judgement on the purpose of the user, which in turn presents numerous difficulties.[43] First, there is no universal, all-encompassing definition of dual use that ignores a subjectively defined purpose. Second, the use of purpose-based dichotomies makes divorcing any possible definition from a case-by-case judgement of particular circumstances, and possibly political or economic expediency, rather difficult. Third, this exposes regulatory regimes of dual-use knowledge, items, and technology to securitisation-driven regulation, thereby drawing into the field of such regulation the geopolitical and geoeconomic concerns of the national regulator beyond purely normative (black letter law) content.

A tempting proposition for treating the issue at hand would be to dispense with the notion of dual use, as some international instruments cited above do, and concentrate on the affected knowledge, items, and technology. This solution, however, presents its own risks as it tends to result in "leaky" proscription lists, especially if tailored too tightly around extant information. Therefore, it would exclude emerging disruptive technologies, at least until a periodic review of the lists of proscribed knowledge, items, or technology is duly undertaken, a problem that, as I shall show below, is currently present, especially in the (non)regulation of dual-use artificial intelligence algorithms. Conversely, a general list of proscribed objects would result in stifling trade, even when dual-use risks are minimal or non-existent. Finally, the creation of global and regional governance regimes, complete with institutions that would determine the dual-use potential of knowledge, items, and technologies through a transparent procedure administered by a court or arbitration body, would be desirable. Such proposals merit consideration by national regulators and international organisations.

3. Major regulatory regimes applied to dual-use technologies

Governance and regulatory regimes applied to dual-use technologies can be classified as either *multilateral* or as *unilateral* regimes. The first is characterised by some form of cooperative adoption and enforcement, even if the regime itself is based on soft law, that is, non-binding instruments. The second is based on the national instruments by which the desired export controls are achieved. While unilateral regimes abound in the field of dual-use technology regulation, multilateral regimes have historically proven to be more efficient tools for preventing the undesired proliferation of technology and providing regulatory templates for unilateral regimes.

43 I would also like to note here that the definition seems to ignore forms of non-desirable use, other than military use, even if such forms, including infringements of human rights, result in inadvertent but possible existential risks.

An example of such multilateral solutions and arms control regimes is the well-established element of the international legal order. Binding and nonbinding instruments with the scope of preventing the proliferation or development of WMDs abound and have existed for a considerable amount of time (at least since the 17th century).[44]

Numerous such instruments, especially those adopted beginning in the second half of the 20th century, many of which will be mentioned in this respect in the following, usually contain some provisions regarding dual-use knowledge, items, or technologies, even if the notion of dual use itself is not explicitly mentioned in their text. Their stated aim was to enhance global, regional, and national security by restricting the proliferation of knowledge, items, and technologies that were considered to pose significant risks. Such regimes may manifest themselves in binding multilateral instruments, such as arms control treaties (specifically adopted to defend against the spread of weapons of mass destruction or other types of weapons), export restrictions, and other barriers to trade enacted at the regional level, or unilateral measures.[45]

From the perspective of dual-use knowledge, items, and technologies, the first regime which remains relevant today was the result of the (now – possibly – first) Cold War, namely, the establishment of the Coordinating Committee for Multilateral Export Controls (COCOM) in 1949,[46] with various systems instituted in different forms throughout the Cold War and beyond.[47] The establishment of this first specific regime and its maintenance during the Cold War also occurred with the intention of stunting technological development in countries that were considered hostile to the United States (US).[48] Therefore, it constitutes an eloquent example of a multipurpose regime that serves national security objectives, as well as economic and political leverage in the form of an embargo. The COCOM regime later evolved into the Wassenaar Arrangement,[49] geared initially – in the climate of cooperation and good will that characterised the end of the Cold War – towards preventing technology transfers to "pariah" states that could pose a significant risk to international order. Following this transformation of the COCOM regime, other dual-use technology control regimes continue to aim to restrict technology transfer in the interest of national security as well as to impose embargos and erect other impediments to international development in the interest of major powers.[50]

The most significant multilateral (legally non-binding but generally adhered to) instruments for dual-use technology export control include the Missile Technology Control Regime, the Nuclear Suppliers Group, the Australia Group, and the

44 Davis, 2002, pp. 20–22.
45 For an exhaustive historical list of such regimes, up to the year 2002, see: Grahame, 2002.
46 See: Bown, 2020, pp. 296–298.
47 I shall analyse the notion of dual use in such later regimes, in more detail in the following.
48 See: Hofhansel, 1993.
49 Kim, 2021, pp. 386–387.
50 Davis, 2002, pp. 32–36.

Wassenaar Arrangement. Of these, the last is the most significant, as the other instruments are either not meant to govern dual-use technologies in general terms and remain limited to the fields of nuclear and missile technology, respectively, or (as in the case of the Australia Group, being confined to the governance of chemical and biological technologies[51]) do not explicitly, or even implicitly, consider all emerging and disruptive technologies.

Unilateral export controls constitute regimes instituted at the national or regional level[52] (mostly implemented by significant geopolitical and economic actors or alliances of such actors) to impede the transfer of (dual-use) technology to potential adversaries and competitors. Export controls may result not only from concerns about the proliferation of weapons or technologies that may be weaponised, but also from the intention to contain or sanction potential adversaries, and even to stifle competition. Unilateral regimes may be set up by significant individual technology exporters such as the US and the People's Republic of China (PRC). It is these two exporters' unilateral regimes that I shall present with particular emphasis in what follows, with the proviso that several other major technology exporters, such as some EU member states, also establish significant export control regimes (by adopting national control lists of proscribed items and/or by adhering to the EU Dual-Use Regulation).[53] Before analysing unilateral regimes, however, the most significant international framework for controlling dual-use items, knowledge, and technologies must be discussed.

3.1. The Wassenaar Arrangement

The Wassenaar Arrangement (named for the small town near The Hague where it was signed) was founded in 1995 by the Final Declaration of December 1995[54] and counts among its members 42 technologically advanced countries.[55] It is by far the most significant multilateral regime for regulating dual-use technologies, and the most relevant when it comes to emerging technologies. Based on this arrangement,

51 The Australia Group, no date a.

52 Here I include EU instruments among unilateral export controls as EU norms, which constitute a complex mesh of rules, which intermingle with national export control regimes and are binding upon the member states just as domestic law would be, while the EU, due to its wider scope, cannot be considered an international organisation in the classical sense.

53 E.g. In the year 2023, the Netherlands, Spain, Lithuania, and Finland adopted such national control lists from among the member states of the EU. European Commission, 2024b, pp. 7–8.

54 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Final Declaration*, 1995.

55 These are as follows: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. Arms Control Association, 2023, n. 1.

the Secretariat instituted by its founding documents publishes and, after considering the feedback from the members, regularly updates the List of Dual-Use Goods and Technologies, and Munitions List.[56] These constitute the proscribed item lists regarding which members agree to institute export controls (implementing a mainly classification-based approach).

Two noteworthy facts should be emphasised. The first is that the Wassenaar Arrangement members include Russia, which in the current security environment is proving extremely problematic when it comes to voluntary compliance,[57] whereas this regime does not include the PRC; the second is that it does not include the EU itself.[58] Even if EU member states are partners in the arrangement, the EU as such is only informally and thus indirectly bound by what is agreed, leaving the content of harmonisation instruments to be determined by a block constituted almost exclusively of members of the arrangement (with the notable exception of Cyprus), without being itself a formal member.

While the arrangement is a sound tool for the control of dual-use technology in general, when it comes to disruptive technologies, it has its shortcomings, as the potential risks and transformative effects of these technologies are not yet known, and many states may desire to progress in developing them. At the same time, the proscribed item lists may not be kept sufficiently up to date to prevent undesired proliferation.

The issue of the PRC's non-participation in the arrangement comes to the fore specifically because of the significant development there related to cyber-surveillance technologies, for which the PRC is also a significant exporter. The arrangement was updated for specific categories of surveillance technologies in 2012–2013, such as systems permitting intrusion into the targeted information technology infrastructure (including mobile telecommunication interception) and internet providers' surveillance tools.[59] However, this was not done with reference to human rights or their possible infringement through the use of mass surveillance, but from traditional defence considerations.

In addition, while the necessity of the arrangement's adaptation to dual-use technologies in general has long been known,[60] and the participating states set out to

> focus on novel or rapidly evolving technologies such as quantum computing, additive manufacturing, suborbital vehicles, advanced sensors, robots and artificial

56 The second volume of these lists is published. For the latest list, see: The Wassenaar Arrangement Secretariat, 2023.

57 The fact that Russia aims to implement dual-use technologies in its military industrial development programmes is quite well known, and even openly stated, and has been so for a long time. See, for example: Bzhilianskaya, 1996.

58 Bown, 2020, p. 298.

59 Kim, 2021, pp. 389–394.

60 Himmelfreundpointner, 2017, p. 65.

> intelligence [considering the Arrangement] as the appropriate forum in which to address trade and security challenges arising from new and emerging technologies,[61]

no notable progress has been made in this regard. However, of the disruptive new technologies, quantum computing is indirectly considered, as the 2023 edition of the Wassenaar Arrangement lists includes technologies that may be utilised to harden or defend cryptography during and after the advent of quantum computing[62] (post-quantum encryption), which would compromise the prime factor-based cryptosystems widely used today.

In addition, while the Wassenaar Arrangement is the gold standard in the domain of multilateral instruments governing the non-proliferation of some dual-use technologies, the technical approach it takes is subject to criticism, as it employs proscribed items lists agreed upon unanimously by the participant states. Such agreements are reached through time-consuming negotiations and therefore may be problematic, as it is necessary to update the arrangement in response to unpredictable advances in disruptive technology, a shortcoming that is already evident with respect to artificial intelligence, as an element of a wider debate[63] on updating the agreement to cover cyber weapons.

Further, the arrangement does not provide for efficient catch-all tools, as it does not result in the adoption of a commonly agreed-upon list of suspicious entities (which would mention end users to whom exports are prohibited) or similar documents, which other mostly unilateral tools utilise. Therefore, while the arrangement is useful as intended against pariah states it is less so against geopolitical adversaries or competitors, a major goal for the development of other dual-use technology regimes, which remain instituted mostly by way of unilateral instruments, even if coordinated at the level of various ad hoc coalitions or alliances.

3.2. The US export control regime

The US operates a complex and comprehensive export control regime[64] comprising several systems or layers of regulation. The rules of the regulatory regime are not limited to what would be considered exports in the common sense of the notion, regarding knowledge, items, or technologies, but also cover so-called deemed exports, i.e. disclosures of information, or release of technologies inside the US to a

61 Griffiths, 2019, p. 4.

62 The Wassenaar Arrangement regulates “post-quantum, quantum-safe or quantum-resistant” algorithms. The Wassenaar Arrangement Secretariat, 2023, p. 95.

63 Ruohonen and Kimppa, 2019, pp. 175–183. The arrangement’s proscribed items list does refer to “military offensive cyber operations” but not specifically to cyber weapons used for surveillance and suppression of human rights.

64 For an overview and critique of this system, see: Congressional Research Service, 2020. See also: Congressional Research Service, 2021.

foreigner, including in situations of academic discourse and scientific communication.[65] One of these layers is constituted by the International Traffic in Arms Regulation (ITAR),[66] which governs weapons and related military-use technology exports (which are not included under the dual-use category). More significant, from the perspective of this chapter, is the Export Authorization Regulations (EAR),[67] through which the Bureau of Industry and Security (BIS) of the US Department of Commerce historically regulated less sensitive technology (not evidently destined for military use).[68] This historic and somewhat limited scope of regulation has been extensively revised since 2018[69] and now constitutes the principal instrument of dual-use technology export control, affecting US-first exporters and foreign re-exporters alike (as well as some participants in US domestic commerce). Therefore, this regulation can be applied extraterritorially. The 2018 iteration of the export control rules constitutes the implementation of a strict, unified regime for the administration of the exports of dual-use technologies (in the civilian–military dichotomy), which follows a wave of moderate deregulation after the end of the Cold War to prevent hindering US exports and as a means of increasing American competitivity with other economies.

Today, the EAR mainly regulates the export of dual-use knowledge, items, and technologies subject to export controls specific to civilian (or at least non-military) implementations, constituting the cornerstone of the Dual-Use System for export control.[70] The scope of the Dual-Use System extends to 'commodities, software, or technologies that have both civilian and military applications'.[71] The system was administered under the Export Control Reform Act of 2018 (ECRA),[72] which ultimately imposes export restrictions on dual-use technologies within the powers of the executive branch, and more specifically, the president of the United States.[73] Determining which dual-use technology exports will be subjected to export controls, however, mainly falls under the jurisdiction of the BIS.

The scope of the US export control rules is established by enumerating the technologies to which they refer (without defining any form of dual use). As novel provisions of ECRA, when compared to the previous regime, and in response to

65 Weinberger, 2009, p. 156. The author points out that deemed exports are vaguely and generically defined, a conclusion valid even in light of the current regulatory regime. See: *Deemed exports*, no date.

66 *The International Traffic in Arms Regulation (ITAR)*, 2024.

67 *Export Authorization Regulations (EAR)*, 2024.

68 See: Alavi and Khamichonak, 2017, p. 67; Lazarou and Lokker, 2019, pp. 2–3.

69 Whang, 2021, pp. 19–20.

70 See: Congressional Research Service, 2020, pp. 2–4.

71 Congressional Research Service, 2020, p. 1.

72 *Export Control Reform Act of 2018*, 2018, secs. 2, 115.

73 For a description of the current provisions of the Export Control Reform Act of 2018, see: Congressional Research Service, 2021.

the growing (but by no means recent[74]) unease about geopolitical and geoeconomic rivalry with the PRC,[75] the act contains separate measures for emerging and foundational technologies (also named in the act as emerging critical technologies), by creating an interagency process under the supervision of the president of the US, to identify and regulate the export of such technologies. These technologies, pursuant to the ECRA, may be added to the Commerce Control List (sometimes also referred to as the BIS list), a solution that was previously applicable to less sensitive dual-use technologies.

While the act in force does not specifically enumerate the technologies to which this enhanced regime applies, according to the BIS, these should include technologies such as[76] additive manufacturing (popularly known as 3D printing), advanced computing technology, advanced materials (including nanomaterials), advanced surveillance technology, artificial intelligence and machine learning-related technologies, various biotechnologies, brain-computer interfaces, data analytics technologies, hypersonic technologies, (advanced) logistics technologies, microprocessor technology, position, navigation, and timing technologies (e.g. global positioning systems), quantum information and sensing technologies, and robotics.[77] Along with the possibility for the BIS to compile lists of proscribed items, the ECRA provides for administrative licencing of potentially dual-use exports (but also of foreign direct investment in situations where it might provide access to such technologies – a solution that blurs the lines between export controls and investment screening). During the licencing process, the presence of foreign entities or persons who would be considered a threat to US national security is also examined, and considered along with risks presented by the export to the US defence industrial base either in the form of a penury of the exported item, or based on broader economic concerns, such as a reduction in the US domestic production of items, the development of which was funded by federal resources, or the reduction of employment of persons with skills critical to national security within the US.[78] Due to the relative inability of the World

74 The US has been hostile to what it perceives as the "rise" of China and Chinese technological development for decades, citing reasons of economic competition, perceived as significant from the national security and technological superiority perspectives, demonstrating the securitisation of economic competition. See: McCormick, 2006; *Officials Show Scant Interest in Major Export Control Overhaul for China*, 2011.

75 Whang, 2021, p. 26; Gehrke and Ringhof, 2023b.

76 Congressional Research Service, 2021, p. 20; Tongele, 2022a, 2022b. A much wider list of technologies was considered as subsets of the ones listed above. See: Industry and Security Bureau, 2018.

77 Other technologies were added to this list, resulting from the 2019 update of the Wassenaar Arrangement, these being: 'hybrid additive manufacturing (AM) / computer numerically controlled (CNC) tools; computational lithography software designed for the fabrication of extreme ultraviolet (EUV) masks; technology for finishing wafers for 5nm production; digital forensics tools that circumvent authentication or authorisation controls on a computer (or communications device) and extract raw data; software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider via a handover interface; and sub-orbital craft.' Congressional Research Service, 2021, p. 21.

78 Congressional Research Service, 2021, p. 24.

Trade Organization's (WTO's) General Agreement on Tariffs and Trade (GATT[79]) system to combat de-globalisation through the securitisation of world trade,[80] this system allows for provisions (Art. XXI(b)(ii) of the GATT in the 1994 version of the text) that permit the restriction of trade in case of shortages and for the defence of national security virtually without restriction, enabling the US to pursue a wide-ranging geoeconomic programme using export restrictions.

Therefore, the extant US export control regime, and specifically its new post-2018 provisions under the ECRA, aims for more than controlling dual-use technology outflows to protect national security imperatives. In fact, the regime instituted reflects what can be considered as a new, wider notion of economic security, or, more precisely the 'securitization of economic policy',[81] an attempt to maintain and enhance technological and economic advantages over not just adversaries such as the PRC,[82] but also simple competitors.[83]

The US export control regime also doubles as a de facto sanction regime, as the BIS maintains an Entity List,[84] which, unlike the proscribed technology lists, and specifically the control lists of the Wassenaar Arrangement referred to above, does not regulate dual-use knowledge, technology, or items in particular, but the entities to which exports of such items are effectively banned or subject to special conditions. This list contains numerous legal and natural persons, not just from states subject to sanctions but also from EU member states, thereby effectively hindering trade with the EU (albeit within the remit of US economic relations with EU member states).

The US unilateral export control regime effectively operates as an offensive geoeconomic tool[85] (not just as a simple sanction regime or embargo) because of the extraterritorial application of its rules: products that are manufactured outside the US but with export-restricted technology remain subject to it even if the products themselves do not incorporate restricted technology. In this manner, the US may leverage, and is known to have leveraged,[86] its technological might to interfere in commerce between third parties.

79 The name is the abbreviation of the General Agreement on Tariffs and Trade, 1947.

80 Bown, 2023.

81 Bown, 2020, pp. 287–289; Hrynkiv, 2022. The cited author sees the reasons for this securitisation in the transformative effects of digitalisation, and especially artificial intelligence, which increases competition between nations, and threatens to disrupt previous global economic and power hierarchies. In this context, export controls aim not only to defend national security, but also have a broader economic and technological supremacy over perceived adversaries, constituting a manifestation of deglobalisation, when coupled with other, apparently purely economic measures (such as politically, rather than economically motivated tariffs).

82 Bown, 2020, pp. 289–292.

83 Pillar, 2023.

84 For the current entity list, see: *Supplement No. 4 to Part 744, Title 15. Entity List*, 2024.

85 Bauerle-Danzman and Meunier, 2024, pp. 9–13.

86 See: Fägersten et al., 2023.

From these norms, it may be discerned, as has been duly observed,[87] that for geoeconomic reasons, the US desires to decouple from the PRC and acts to preserve and increase American advantages in the high-tech sector (currently specifically semiconductors), with possible adverse effects on the trade position of the EU and its member states.[88] Specifically, unlike the EU, the US utilises its export control regime in a punitive manner to impose specific sanctions on adversaries such as the PRC, while the EU adopts a country-neutral regime combined with specific sanctions to control the export of dual-use technology to states such as Russia.[89]

3.3. The EU dual-use regulation

The EU operates an export control regime comparable in complexity to that of the United States, which is meant to hinder the export of dual-use technologies, to enforce the international obligations of the member states pursuant to non-proliferation instruments adopted under the aegis of the United Nations (such as the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention, the Biological Weapons Convention, and UN Security Council Resolution 1540), to comply with international soft-law instruments that set up multilateral export control regimes, and to implement EU foreign policy measures, including various sanctions.[90] This regime is underpinned by the recently recast comprehensive Regulation (EU) 2021/821[91] (EUDUR). The EU dual-use technology regime may well be considered as a multilateral instrument, as, while the EU does have a legal personality under international law, its regulatory powers extend to member states.

Regulation (EU) 2021/821, as the previous applicable norm, does not stop member states from adopting dual-use technology export controls of their own, insofar as they do not contradict the provisions of the EU norm, a behaviour that has resulted in undue complications in determining applicable norms, and the risk of a "patchwork" legal regime.[92] According to the EUDUR, member states are beholden to enforce all international sanctions obligations, arising from '(…) sanctions imposed by a decision or a common position adopted by the Council or by a decision of the OSCE or by a binding resolution of the Security Council of the United Nations' (Article 15(1)(b), see also Recital no. (19)).

87 Gehrke and Ringhof, 2023a, 2023b; Fägersten et al., 2023, pp. 6–7.
88 Fägersten et al., 2023, pp. 55 et seq.; Chorzempa and von Daniels, 2023.
89 Gehrke and Ringhof, 2023b.
90 See: European Commission, 2024a.
91 *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*, 2021.
92 European Commission, 2024b, p. 8. To document national export controls for dual-use technology, the European Commission on 20 October 2023 published a list of national export controls. See: European Commission, 2023.

The specific solution for dual-use technology export control adopted by the EU is tailored to the structure of the EU itself, and therefore serves as a harmonisation instrument. The EUDUR creates a set of common rules for exports, including technical assistance and transit of items subject to export restrictions, of dual-use technology, as well as common criteria based on which the exports are to be assessed and authorisations are to be granted, common end-use controls, and catch-all rules for non-listed items (e.g. that may be used to restrict human rights in the course of cyber surveillance, or the manufacture of WMDs).[93] This part human rights-based approach, especially regarding the catch-all clause governing the export of technologies prone to use in cyber surveillance (to which I shall refer below during the discussion of dual-use AI), constitutes a specific aspect of the EU export control regime and one that was not universally accepted at the outset, in part because it placed the onus of vetting potential export destinations on the exporting entity, usually a private company.[94]

The EUDUR is the result of a recent trend in the EU, dictated by the European Commission, which has the aim of mobilising the bloc towards proactive participation in geoeconomic rivalries. in the post-2017 context of US–PRC tensions, tendencies for disengagement from multilateral organisations by the US, an increase in economic protectionism, and risks such as the Covid-19 pandemic and the flareup of the Russo–Ukraine war. In short, the regulation stems from the EU's intention to follow suit in the increasing securitisation of economic relationships by creating offensive and defensive geoeconomic tools, among which export controls occupy a significant position.[95]

This, especially with regard to the PRC, is in stark contrast to the pre-2017 period, during which, in the lack of any major security interest in the Asia-Pacific region, the EU placed emphasis on Eastward-bound trade and cooperation, while observing existing export restrictions, such as the arms embargo instituted against the PRC after 1989.[96]

This period ended in a series of near-collisions between EU and US policies towards the PRC, in which the US demonstrated a high degree of commitment towards securitising trade relations, and as part of a wider pressure campaign to force US allies to choose sides in the Indo-Pacific region's disputes, strong-arming the EU into adopting policies contrary to the initial intentions of the bloc, such as discouraging several EU member states from participating in the Asian Infrastructure Investment Bank or the Belt and Road Initiative.[97]

This demonstrates that centripetal forces in action between the US and the PRC are pushing the EU towards adopting measures, including in the domain of export

93 See: European Commission, 2024a.
94 Kanetake, 2019, pp. 159–161.
95 Bauerle-Danzman and Meunier, 2024, p. 13.
96 Bräuner, 2013, pp. 460–461.
97 Deng, 2020, pp. 113–118.

regulation, that now run counter to initial attempts at establishing interconnectivity and rare dictated by developments in a region that the EU, for a long time, prior to US-driven securitisation of economic relations – considered as one outside its sphere of strategic interest, as merely a partner and economic competitor, but not a security threat.[98]

The EU export control regime may be considered as long-suffering from various maladies that the recast version of the EUDUR (as well as previous iterations of its rules) has only partly addressed, such as difficulties in the mutual recognition of export licence documentation, the problems of firms established in several member states in correlating and adhering to the various national regimes, along with the common EU regime, and the information flow regarding end users of the exported technology, which is crucial for operating the catch-all rules of the regulation.[99] Some of these difficulties were partly addressed;[100] however, the current state of the regulation has not been immune to criticism (especially when it comes to transparency and the possibility of member states "taking over" measures adopted by other member states, a particularly pernicious problem if a common defence market is to be achieved). This criticism was levelled against several aspects of the EUDUR as follows:

1. The regulation continues to be a patchwork system, with a wide range of possibilities for member states to institute their own controls, parallel to the EU framework, a problem that is compounded by the fact that that these frameworks, in spite of the publication of a compilation of national rules in late 2023, lack transparency and are developed without sufficient consultation.
2. If member states decide to adopt (take over, as a measure permitted by the regulation) and implement controls previously enforced by other member states, there is little communication about when and how this may occur, a problem that particularly impacts catch-all measures specific to unilateral sanctions, which should be (but are not being) efficiently disseminated between the exporters of the various member states.
3. Member states may be barred by domestic rules from adopting export controls from other member states.
4. Forum shopping may occur when products cannot be directly exported from a given member state to a third country, but after transfer to another member state with more lenient rules for dual-use technology export, such an export may commence.
5. The lack of a common set of overall objectives in the field of export control policy, as member states hold the initiative in defining the contents of what is basically a multilateral regime (a problem that the White Paper on Export

98 Bauerle-Danzman and Meunier, 2024, p. 7.
99 *Chopping the Red Tape*, 1998, pp. 4–5.
100 *United States: Proposed Changes to the EU Dual-Use Export Control Regime*, 2016.

Controls proposes should be solved by extracting this domain from the ordinary legislative procedure).

6. The lack of common EU action internationally, as part of the EU common foreign and security policy, which also exposes some member states to strong-arming, even from partners.[101]

Thus, the EUDUR is an imperfect instrument that should be updated, keeping in mind the creation of a common set of EU-administered export rules, constituting a unified regime that may also benefit the common defence market currently taking shape.

3.4. The PRC's export control regime

Chinese policy on the development of civilian–military dual-use technology has shown significant novelty in recent years. Both direct and indirect instruments adopted in this area have increased in number and significance, starting in 2001, with a noticeable wave of regulation from 2015 to 2020. It demonstrates a policy trajectory towards enhanced bi-directional (military-to-civilian sector and civilian-to-military sector) technology transfer, as well as technological integration between military and civilian applications, including by breaking down confidence barriers between the military and civilian sectors, and by establishing common standards.[102]

This change in stance can be attributed to the broader set of policies enacted to achieve a wider economic transformation, by relying on emerging and transformative (digital) technologies as the drivers of future economic growth. The overall objective is avoiding the "middle income trap" that threatens the current structure of the PRC's economy.[103] Therefore, the PRC's efforts to attain a leading position in emerging and transformative technologies constitute more than a simple drive for modernisation, of which there have been many in the nation's history; they are driven by an imperative set in the strategic context of geopolitical rivalry. This perception stems from an expectation on behalf of PRC policymakers towards interference by the USA and other Western powers directed at the economic containment of the PRC,[104] which has, from the Chinese perspective, been partly realised by concrete measures, particularly those enacted by the US, directed against the export of technologies vital to the PRC's aspirations.

In response to measures undertaken by the US in the context of what is perceived on both sides of the Pacific as a wider geopolitical and geoeconomic rivalry (inter alia, by targeting PRC-registered companies for mixed, partly politicised reasons),

101 European Commission, 2024b, pp. 8–12.
102 Meng and Wang, 2023.
103 Qi and Chu, 2022, pp. 19–23.
104 Qi and Chu, 2022, p. 16.

the PRC has also enacted its first Export Control Law[105] (known as the ECL, replacing under this respect the less detailed provisions of the Foreign Trade Law), which came into force in 2020. Dual-use items are specifically mentioned as within the scope of this law, as well as a catch-all category comprising 'technologies, services and items relating to the maintenance of national security and national interests' (which constitute a novel element of the rule as opposed to the previous governance regime).[106] The ECL places the onus of identifying dual-use knowledge, items, or technologies subject to export control on the exporter. While the PRC's government does provide some lists of proscribed items, due to the lax formulation of the provisions of the law, its material scope may even be arbitrarily extended to other knowledge, items, or technology during the applicable administrative procedure when exporters apply for a licence.[107] During this procedure, the effects of granting the licence must also be examined, inter alia on considerations of national security and national interest, as well as on the "sensitivity" of the exported item itself.[108]

The export control regime instituted in the case of dual-use technologies by the PRC, dominated by the state in its administrative capacity, lends wider leeway to abuse than the previously examined systems, as the exporter is left to establish compliance mainly by its own devices, but it should be noted for its ability to rapidly adapt to changing technological realities.

4. Control regimes of some emerging dual-use technologies

The wide range of foundational, emerging, and disruptive dual-use technologies mentioned above require regulation to prevent major, even existential risks, not only to national but also global security, and to achieve non-proliferation. Therefore, not all such technologies may constitute the object of our analysis, and subjective selection is inevitably required.

This selection, while subjective, should at least partly consider the impact of the given disruptive dual-use technologies in the present and near future. Based on this criterion, in the following, I shall assess the specific regimes applicable to artificial intelligence, adjacent electronic processing (semiconductor technology), biotechnology, and 5G, leaving some other technologies, which I believe shall also have a serious impact later, to be analysed at another future occasion.

105 The State Council of China, 2021.
106 Köstner and Nonn, 2023, pp. 82–83, 87. The similarity with the US dual-use export regime should be noted here.
107 Köstner and Nonn, 2023, p. 92.
108 Köstner and Nonn, 2023, p. 92.

4.1. Artificial intelligence, advanced semi-conductor technology and quantum computing

Artificial intelligence (AI), considered one of the most important dual-use technologies under development, with a potentially transformative effect on most aspects of human existence, not only in the domain of information technology, but also in biotechnology and even warfare using dynamic weapons, constitutes one of the most significant objects of dual-use technology regulation, which is increasing in depth and volume.[109]

Several use-cases of AI being quite similar if not entirely identical in civilian and military applications (e.g. a self-driving "car" may very well be, in fact, also an armoured vehicle), the percolation of civilian AI development into the military field, along with robust research and development for exclusively military applications are a foregone conclusion. Considering the possibility of such diffusion, although some studies have shown that it is not (yet) very significant,[110] it is reasonable to assume that AI should constitute a major object of regulation meant to impede the free flow of technologies, specific items (e.g. microprocessors), and specialised knowledge.

In the case of AI, concerns of civilian technological advances being used for military purposes (according to the common dichotomy used to define dual use, especially from the European perspective) have been accompanied by concerns that some states (such as Russia or the PRC) or other non-state actors may view this technology through a different ethical prism, with less emphasis on basic human rights and freedoms, which may in turn facilitate utilising AI as a new, and from their perspective, very useful tool for social control. In this context, the expected utilisation of AI, although not a "classic" case of dual use, as the implementation nominally remains in the civilian (e.g. law enforcement) sphere, may also prove problematic and even threatening.[111]

It should be noted here that while dual-use technology regulation is nothing new, the regulation of AI-related items in the form of export controls, most definitely, is, as part of a renewed push, primarily by the US, to maintain its technological superiority over perceived adversaries,[112] a policy change that became more visible after the 2018 reform of US export regulations, as discussed above.

The restrictions on AI are by no means prompted exclusively based on trade and economic securitisation, or even human rights considerations, as the need for a new form of arms control is becoming more acute,[113] with cyberspace now considered a new and utterly different battlefield. While multilateral arms control

109 See: Ambrus, 2020; Top 10 Emerging Technologies Steering Group, 2023.
110 See: Schmid, Riebe and Reuter, 2022.
111 Schmid, Riebe and Reuter, 2022, pp. 2–3.
112 See: Shagina, 2023.
113 See: Dumbacher, 2018.

may be a modality by which AI, as an emerging technology, may be kept in check in the future, other means, such as export controls, are already being deployed in an attempt to manage risks, including misuse of AI to infringe on human rights, and also 'global security risks if democratic nations lose their current lead in AI'.[114] Assertions such as this make it clear that the ideological argument for technology control in the case of AI rests on a heterogeneous basis, including the maintenance of one trade bloc's advantage over others, or, as seen from Europe,[115] the maintenance of US advantage over all, even at the cost of subverting the global free trade system and the WTO (GATT) regime that was once at its core.

The regulation of dual-use AI technology is inconceivable without regulation of the processing equipment required to attain and operate it, which is why numerous measures for controlling advanced semiconductor exports and proliferation are practically aimed at technologies upon which AI implementations are based. Several export control targets must be considered for AI. These include general AI software, untrained algorithms and open-source datasets, specific AI software, trained algorithms and sensitive datasets, AI chip manufacturing equipment, and manufactured AI chips.[116]

Establishing a regulatory regime for AI has been the object of a major effort by the EU.[117] Finally, in a momentous act of legislative prowess, the EU AI Act (in fact a regulation according to the structure of EU instruments) was adopted.[118] It is noteworthy that while most risks of the use and abuse of AI were considered during the preparation of the AI Act, the problems of dual-use and export restrictions were not regulated. This may be explained by the scope of the instrument: the AI Act was specifically not meant to apply to military activities or the domain of national security (Recital (12a) and Article 2(3) of the Final Draft). While the act itself is intended to enforce human rights protection objectives, the notion of human rights is mostly omitted (except for the Recital (60m) of the final draft regarding artificial general intelligence).

This is not so in the US, where, partially as a reaction to the adoption of the AI Act, an Executive Order[119] was issued that explicitly refers to dual-use foundation models and their regulation (including exports and proliferation). Foundation

114 Flynn, 2020, p. 2.
115 Herrmann, 2023, pp. 2–4; Bauerle-Danzman and Meunier, 2024, p. 13.
116 Flynn, 2020, pp. 6–9.
117 For the most significant preparatory materials, see: Independent High-Level Expert Group on Artificial Intelligence, 2019a, 2019b, 2020b, 2020a.
118 The text of the Act has not been published in the Official Journal of the EU at the time that the manuscript of the present chapter was finalised. For the final draft, see: European Commission, Directorate-General for Communications Networks, Content and Technology, 2024.
119 The White House, 2023.

models constitute the essence[120] of generative AI, allowing "trained" algorithms to be applied to real-world situations, resulting in AI-generated feedback. This notion is also absent from the EU AI Act.

The EUDUR (with its content inspired by the Wassenaar Agreement regime) does not consider or regulate exports in the form of trained or untrained broad-purpose AI algorithms (such as machine learning or other algorithms implemented on hardware capable of operating neural networks), whereas it regulates specific algorithms for other uses in several situations (including cryptography and equipment operation). The regulation does govern exports of hardware that may be used for AI purposes (under items such as '3A001 – Electronic items', or '4A004 – Computers as follows and specially designed related equipment, "electronic assemblies" and components therefore').[121]

The EUDUR also implicitly governs the export of AI technologies (which in this case do include trained algorithms), through the interoperation of Article 2(1) (the definition of dual-use items, which includes software), Article 2(20) (which separately defines "cyber-surveillance items" as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems') and the catch-all clause at Article 5(1), which requires authorisation for cyber-surveillance items not specifically listed,

> if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.[122]

120 A very recent definition of foundation models establishes the meaning of the term as follows: 'Foundation models constitute large-scale AI models that are pre-trained on vast amounts of general data and that can be adapted for downstream applications (e.g., by fine-tuning them through further training on application-specific data). Through this pre-train and adapt approach they expedite the development of innovative AI products and services and accelerate the accessibility of high-performance AI solutions in various industries (…). Foundation models show remarkable abilities to comprehend, generate, and adapt content across diverse domains, including creative generations (…), software debugging (…), protein sequencing (…), or cross-modality outputs such as text-to-image creations (…). With scaling, foundation models are becoming increasingly good at performing tasks they were not explicitly trained for, thereby broadening the scope of applications achievable by a single model without the need for additional training data or fine-tuning (…). When needed, task-specific performance can be further enhanced through fine-tuning or effective prompt engineering techniques; both of which incur significantly lower costs in comparison to developing a new model from scratch (…)'. Schneider, Meske and Kuss, 2024, p. 221.

121 The technical note of the EUDUR at item 4A004 reads as follows: 'For the purposes of 4A004.b., "neural computers" are computational devices designed or modified to mimic the behaviour of a neuron or a collection of neurons, i.e., computational devices which are distinguished by their hardware capability to modulate the weights and numbers of the interconnections of a multiplicity of computational components based on previous data.'

122 See: Vandenberghe, 2021.

In an approach that sets US regulations only slightly apart from the European model, the BIS specifically establishes restrictions on disruptive technologies, which include AI, with a view to strategic competition with the PRC (even if such restrictions are again centred mostly on hardware components and specifically microchips, that is, semiconductors, of a given ability),[123] a solution present in the EUDUR.

Such restrictions have been recently updated to include several new export control items:

> (…) 3A090, which concerns some advanced ICs that can have transfer rates of 600 gigabytes or more, (…) 3B090, which concerns semiconductor manufacturing equipment and related items, (…) 4A090, which concerns computers, assemblies, and components that include integrated circuits (ICs) over the limit delineated in 3A090a (…) 4D090, which concerns software tailored to developing items controlled under 4A090.[124]

Manufacturing equipment[125] for such advanced semiconductors is also the target of export restrictions.

These restrictions are dispersed and the Commerce Control (BIS) Lists,[126] true to the Wassenaar Arrangement model, only refer to processing equipment and encryption algorithms. The above-mentioned Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence covers algorithms but does not yet specifically regulate the export of general-purpose AI algorithms.

This approach (prevalent in the literature between 2017 and 2020) is accredited in theory by considering that general-purpose AI algorithms would be harder to regulate, and the choke-point that should be targeted by dual-use technology export regulations, is primarily the semiconductor industry.[127] However, this method of regulation tends to ignore recent and dramatic advances in generative AI (such as ChatGPT), which, although having a general purpose, shows impressive potential as a direction for technological development.

The focus on advanced semiconductors and computer assemblies (as well as only some specialised algorithms) by the EU and US regulators alike, with the EU rules enhanced by human rights protection clauses, begs the question of whether a catch-all clause would have to be included in the norms, to extend the rules to general-purpose AI algorithms, as well as some commonly recognised threat actors, to permit cooperation and create an environment in which free trade and security concerns may coexist, as much as possible.

123 Bureau of Industry and Security, 2022, 2023a.
124 Reinsch, Schleich and Denamiel, 2023.
125 Bureau of Industry and Security, 2023a; *The United States Announces Export Controls to Restrict China's Ability to Purchase and Manufacture High-End Chips*, 2023.
126 See: Bureau of Industry and Security, 2024a, 2024b, 2024c.
127 Flynn, 2020.

Another potential problem is the use of AI in cyberweapons, such AI algorithms could be subject to rules on military technology exports[128] if they are clearly incorporated into such technology, but otherwise, and unless their purpose is clearly military, they may escape regulation altogether.

With major export control efforts directed at containing the proliferation of advanced semiconductor technology, another aspect is overlooked and perhaps more difficult to control by either the US or EU export control regimes. Human resource migration towards states (particularly the PRC), which are the subject of clearly stated or thinly veiled measures aiming to control the flow of certain dual-use technologies, is difficult to subject to similar "export" controls as hardware components and manufacturing technologies.[129] Without considering the flow of human resources, dual-use technology regulation as a singular measure may be necessary but by no means sufficient for the stated aims of containing the complex set of technologies that result in AI applications, even if the notion of "export" is usually defined to include revealing sensitive information (as in the case of deemed exports).

A specific field adjacent to AI, which should be mentioned owing to its potentially transformative nature and significant dual-use potential, is quantum computing. While not a discipline strictly linked to AI, quantum computing may result in revolutionising different aspects of information technology in the fields of encryption and communication, rendering most modern techniques of encryption useless, and permitting forms of communications that through a phenomenon known as quantum entanglement results in instant, tamper-proof communications, possibly over incredible distances; quantum metrology also presents significant dual-use potential as developments in this field may lead to highly enhanced location sensors.[130]

While the Wassenaar Arrangement regime, and thus the EU and US export control regimes,[131] also envisage some software applications that would either be implemented on quantum computing systems or would be immune to the impact of such systems on traditional means of electronic encryption, neither of these regimes currently refers to specific quantum computing hardware, as the technical characteristics of such hardware would be difficult to grasp and discern at this moment. Therefore, as stated in the literature and in a manner somewhat similar to the case of disruptive biotechnologies discussed below, soft-law methods of governance, such as codes of conduct and voluntary compliance programmes, are possible methods for preventing the proliferation of dual-use quantum computing.[132]

128 Herr and Rosenzweig, 2016.
129 Chu, 2008.
130 Johnson, 2019.
131 E.g. At item 5A002. *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*, 2021; Bureau of Industry and Security, 2024b.
132 Johnson, 2019.

4.2. Biotechnology

Biotechnology (and its various subfields, such as genetics, genomics, biochemistry, virology, bacteriology, and biology-related nanotechnology) is a complex subject of regulation. Entry limits in the biotechnological domain are far removed from the difficulties posed by past disruptive technologies, such as nuclear weapons systems (although such impediments are still more consistent than those for information technology). In fact, with increased globalisation of both knowledge and technological means to affect biological and biochemical research (in this field, often referred to as dual-use research of concern, abbreviated as DURC), a completely new set of absurdly dangerous dual-use scenarios has emerged. These include the laboratory synthesis or enhancement of dangerous pathogens, such as the machine-based generation of the 1918 influenza virus, of various poxviruses, or artificially increasing the transmissibility of the H5N1 zoonotic influenza virus between mammals, or AI-aided discoveries for the manufacturing of known (and possibly unknown) toxins, such as the VX nerve agent.[133] The advent of CRISPR/Cas9 as a method of reasonably accurate gene editing has added an entirely new layer of risk, as it makes large-scale interventions into the DNA and RNA of existing organisms practically feasible, with the added risk that the proliferation of this technology is not easily controlled.[134] A third layer of complexity is added by combining the above technologies with AI, resulting in machine-learned methods for generating toxins, or enhancing pathogens (gain of function experiments); such combinations render much if not most of the research that makes use of technological synergies, dual-use.[135] These examples underline the interconnectedness of some dual-use technologies, as information technology is integral to modern biotechnological research, with the dangerous prospects of synthetic biology (the possibility of creating or enhancing living organisms, or even new types of organisms that do not exist yet) vastly increasing the risks of unintended consequences, including dual-use scenarios.[136]

Development critical to advancements in medicine and pharmacology usually occurs in the private sector; therefore, voluntary compliance with the regimes imposed for dual-use technology regulation is paramount. However, no such centralised regime is forthcoming; a problem specific to the dual-use dilemma in life sciences seems to be the heightened significance of ethics rules and bodies, along with the lack of a workable definition for dual use[137] (which seems to plague life sciences as much as legal science). The very notion of dual use has gained an entirely new meaning in the field of biotechnology, one which is different from those

133 Urbina et al., 2022.
134 See: Mir et al., 2022.
135 Evans, 2022.
136 For the dilemma posed by publishing the methodology of an experiment aimed at synthetically enhancing the H5N1 strain of influenza, see: Rager-Zisman, 2012.
137 Dubov, 2014.

utilised in the "classical" instruments for governing dual-use technologies.[138] In this domain, "dual use" is not only employed to refer to potential military applications, or even just nefarious applications of a given technology, but also to unethical (e.g. unintended) use in general.[139] Therefore, legal dual-use regimes are doubled in life sciences by science ethics supervision,[140] adding a list of government and academic supervisory bodies (including editorial and ethics boards organised outside clearly defined legal frameworks) and authorities to the regulatory mix, with competences not only regarding the international or domestic (deemed) export of such technologies but also a myriad of other competences and activities.[141]

The promotion of self-regulation in this domain is therefore necessary, at least to complement extant and future sources of law. This solution is also justified by the high rate of voluntary compliance with such regimes, as well as the ability of the private sector to institute consortia that would impose compliance with the standards set, with sufficient assistance from government. This is so, first, to contain non-compliant industry actors and encourage them to join self-regulating bodies and abide by their common rules and practices, and second, to dispel industry secrecy, which would be counter-productive for enforcement.[142]

A multi-tiered approach has recently been proposed for managing the risks posed by dual-use technology development, which is specifically suitable for biotechnology and may be deployed in the stages of early development by scientific institutions, functioning in conjunction with domestic and international normative regimes. According to this approach, self-governing bodies, research funding agencies, regulators, and publishers should all consider the risks posed by the given technology for dual use (including nefarious use), properly screen the personnel researching and operating the technology, share data regarding the participants in dual-use research, consider the results of dialogue with civil society in general when developing directions of research, weigh the need for research with inherent risks to determine future risks and enhance governance, and finally adapt scientific publication practices (including publication in preprints) to prevent undesired knowledge or technologies from being published.[143] As a manifestation of this approach, the World Health Organization, beginning in the early 2010s, examined (though ultimately rejected[144]) measures to suppress the publication of possibly dual-use knowledge regarding some pathogens.[145]

138 Campbell, 2006.
139 Pustovit and Williams, 2010; van der Bruggen, 2012, pp. 745–748.
140 Rychnovská, 2016.
141 A case in point is US academic biotechnology research supervision. See: Fox, 2004.
142 Maurer and Fischer, 2010.
143 Yoshizawa et al., 2023. This approach, as the authors show, would in turn limit the scope of open science. The problem of limiting open science in turn, particularly in life sciences and biotechnology, is treated partly as a philosophical question (see: Selgelid, 2009; 2013), in lack of regulatory input through hard-law instruments.
144 Rager-Zisman, 2012.
145 Stone, 2012.

In enforcing this multitiered approach, the definition of dual use is of paramount importance. One of the best proposed definitions (which only covers research) originates from the American National Research Council of the National Academies' Fink report,[146] which aggregates all definitions of dual use to which I have referred.[147] Thus, the purpose-definition problem of dual-use persists in biotechnology.

Regarding legislative (i.e. soft law, hard law, or black letter law) regimes governing dual use in the life sciences, the Biological Weapons Convention (as the Biological and Toxin Weapons Convention of 1972) did not initially envisage the dual-use problem, perhaps owing to the lower level of interconnectedness in the domain of biological research at the time of adoption. However, after the 11 September 2001 attacks and the associated acts of bioterrorism, this approach was reconsidered, and the Sixth Review Conference of the convention, in its 2006 Final Document,[148] did consider the factors of dual-use items (i.e. pathogens) and knowledge,[149] thereby implicitly recognising the possibility that the convention's regime may be extended to such situations.

The EUDUR, continuing the tradition of previous norms,[150] does not specifically refer to a dual-use regime in the field of biotechnology (the civilian–military dichotomy forms the basis of the regulation as discussed above). However, the EUDUR implements protective measures for some dual-use technologies specific to the field of biotechnology, after its most recent update,[151] such as subjecting to licencing the export of '"Software" specially designed for nucleic acid assemblers and synthesisers specified in 2B352.i., that is capable of designing and building functional genetic elements from digital sequence data' as per Annex I subcategory 2D352 of the EUDUR.[152]

Further, historically the EUDUR has restricted the export of laboratory equipment, which in turn may be of dual use (e.g. under subcategory '2B352 Biological manufacturing and handling equipment'). Some pathogens and substances with biotechnological relevance are also subject to the EUDUR, such as those under the Technical Notes for item 1C353 (e.g. biological agents that would reduce immune responses).[153]

In addition, in the context of European geoeconomic securitisation, significant member states have lowered the thresholds for investment screening (France and

146 Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, 2004; van der Bruggen, 2012, p. 754.
147 See: Selgelid, 2009, p. 176; van der Bruggen, 2012, p. 754.
148 *Final Document of the BWC Sixth Review Conference*, 2006.
149 van der Bruggen, 2012, pp. 743–744.
150 See: Czarkowski, 2010.
151 Raivo and Triščuka, 2023.
152 Subcategory 2B352.i. of the EUDUR refers to 'Nucleic acid assemblers and synthesisers, which are partly or entirely automated, and designed to generate continuous nucleic acids greater than 1,5 kilobases in length with error rates less than 5 % in a single run'.
153 Erbay, 2023, pp. 25–26.

Germany) and have even introduced intra-EU investment screening (Italy and Spain) in the biotechnology sector.[154]

The US BIS proscribed item lists also contain materials and agents that are relevant for the development of biotechnologies and the limited access knowledge required for such undertakings,[155] similar to the EUDUR.

4.3. 5G Communications

In the field of wideband communications, and regarding the technology generally known as 5G, the dual-use dilemma takes a new shape: export controls in this situation become secondary to foreign direct investment considerations, and import controls enacted as part of an effort by the US and its allies to stem the growing influence of the PRC in this sector.

Technological dominance in the field of 5G[156] as a potentially disruptive and transformative emerging technology, also given its possible synergies with other emerging technologies, such as AI, robotics and the "Internet of Things" is considered key in the securitisation of national economies. This field is currently dominated by the US (through domestic 5G chip supplier Qualcomm, and the collaboration between Taiwanese company MediaTek and US-based Intel), with Samsung (South Korea), and Huawei (a PRC-controlled, ostensibly independent company), the other participants in a 'very narrow playing field'.[157] As a manifestation of the push for securitisation of the telecommunications industry, the US and its allies have invoked various concerns, including the possibility of back doors built into 5G systems supplied by manufacturers based in the PRC, but also the unacceptable system of values gaining prominence along with Huawei's technological development, such as online censorship and a breakdown of the openness that should characterise the increasingly liberal global culture, in the name of "cyber-sovereignty".[158]

In the hostile climate generated by the US–PRC strategic competition, and against the backdrop of administrative measures by the US to exclude Huawei and other PRC-based companies from developing domestic 5G infrastructure, significant EU member states such as Germany have found themselves confronted with the dilemma of lining up behind what are essentially trade and investment policies

154 Bauerle-Danzman and Meunier, 2024.

155 See: Bureau of Industry and Security, 2023b; *Deemed Exports and Fundamental Research for Biological Items*, 2024.

156 Bartholomew, 2020.

157 Moore, 2023.

158 Bartholomew, 2020; Moore, 2023. Such concerns are by no means far-fetched as the PRC has taken a leading role in global policymaking when it comes to setting the operational standards of the Internet, and seems to have favoured the adoption of solutions and technical standards that permit a greater control over cyberspace, inter alia by favouring the introduction of state controlled points of access, and a reduction of the fabled anonymity that characterised the Internet's earlier phases of development, including by making the identification of real-world identities of Internet users easier. Yoo and Mueller, 2024.

dictated by US securitisation concerns or following previously laid plans for 5G infrastructure development.[159] Until recently, this dilemma has produced little in the way of a decisive break with Huawei as a leading 5G technology manufacturer; however, a reduction in reliance on this manufacturer's technology in critical infrastructure has been proposed and is being implemented[160] by means of import and investment controls (mostly left in the sphere of competence of EU member states). When it comes to compliance with US requests for exclusion, by legislative means, of Huawei from the development of 5G infrastructure, one recent study[161] has convincingly demonstrated that the positioning of secondary states, such as NATO and EU member states in the US–PRC rivalry is determined by the patron-client theory of international relations, with the most significant factor in rendering a policy response towards exclusion of PRC-based actors from 5G development being the security guarantees granted to a state by the US (this point being validated, including for EU member states).

This said, Germany, as one of the EU's leading economic powers, and a significant actor in EU-level regulation, in a way representative of the entire EU, has adopted a stance of cautious cooperation with US policies,[162] and other measures against the PRC in the field of emerging, and disruptive dual-use technologies, which is likely to determine the fate of 5G development in the future.

5. Conclusions

I have attempted to offer as comprehensive a view as possible, considering the medium used, pertaining to the topic of dual-use technology regulation and the regulatory regime applicable to some major emerging and disruptive dual-use technologies.

In a field dominated by mistrust and rivalry between technological powers, and a wide array of normative instruments, some of a binding nature, others constituting soft law, it may be stated that several considerations interact to create the fuzzy notion of "dual use": military and civilian use, and benign and nefarious use are at the poles of various dichotomies, leading to a combined risk-based approach that emphasises (presumed, or possible) intention. As such, the definitions of dual use in various instruments and regimes only partly overlap, leading to uncertainty as to whether, and more importantly, why, some elements of emerging and disruptive technologies should be considered dual-use, whereas others should not. This

159 Krolikowski and Hall, 2023.
160 Sarah, Andreas and Hakan, 2023.
161 Christie, Jakobsen and Jakobsen, 2024.
162 Cook, Ohle and Han, 2022.

situation is further complicated by the ethics-based approach to dual use prevalent in the fields of molecular biology and related biotechnology, which, in turn, interacts with applied information technology and AI.

The presumed and possible intentions of parties, as well as the geoeconomic interests of some actors in an atmosphere of securitisation of scientific research, trade, and techno-economic development, combine in various unilateral and bilateral instruments to result in governance regimes where considerations for restricting the flow of dual-use knowledge, items, and technologies no longer follow the previous track of avoiding military or nefarious use, while remaining permissive to global trade.

In this environment, the EU, through the EUDUR, an imperfect but useful instrument, has attempted to provide a principal, not just a geo-economic basis for considering the defence of fundamental human rights and freedoms, within a catch-all clause to prevent the misuse of information technology to achieve greater levels of surveillance. In turn, the US has sought to endow economic advantage and technological superiority with national security significance and has tailored its dual-use export regime to maintain this primacy as a manifestation of securitisation. The PRC has followed a similar track, while multilateral institutions and supra-regional instruments have been mostly ignored or sidelined, complicated by geopolitical realities, such as Russia's membership in the Wassenaar Arrangement.

I have shown that both in the field of artificial intelligence, and the related field of biotechnology, regulatory regimes, which do exist in the "classical" instruments of dual-use technology governance, must be complemented by voluntary compliance and ethical standards. Further, specifically in the field of AI, a lack of proper definitions of artificial intelligence, and governance of AI algorithms as dual-use technologies unto themselves is still present (although the "hardware" component of AI systems in the form of semiconductors is highly regulated).

Any future regulator of dual use, including the EU, has to walk a tightrope between overly permissive and overly restrictive norms, something that is problematic in the current environment of strengthening restrictions. Specifically human-rights based approaches, such as those used by the "European model" for restricting proliferation of disruptive, emerging dual-use technologies should be more widely considered as part of such efforts, to the detriment of economic securitisation.

References

Alavi, H., Khamichonak, T. (2017) 'EU and US Export Control Regimes for Dual Use Goods: An Overview of Existing Frameworks', *Romanian Journal of European Affairs*, 17(1), pp. 59–74.

Ambrus, É. (2020) 'Artificial Intelligence as a Dual-use Technology', *Academic and Applied Research in Military and Public Management Science*, 19(2), pp. 19–28; https://doi.org/10.32565/aarms.2020.2.2.

Arms Control Association (2022) 'The Wassenaar Arrangement at a Glance'. [Online]. Available at: https://www.armscontrol.org/factsheets/wassenaar (Accessed: 15 February 2024).

The Australia Group (no date a) *Objectives of the group*. [Online]. Available at: https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/objectives.html (Accessed: 15 November 2023).

The Australia Group Australia (no date b) *Guidelines for Transfers of Sensitive Chemical or Biological Items*. [Online]. Available at: https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/guidelines.html (Accessed: 10 October 2023).

Bartholomew, C. (2020) 'China and 5G', *Issues in Science and Technology*, 36(2), pp. 50–57.

Bauerle-Danzman, S., Meunier, S. (2024) 'The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator', *JCMS: Journal of Common Market Studies*, 62(4); https://doi.org/10.1111/jcms.13599.

Blanken, L.J., Lepore, J.J. (2024) 'Trade Policy for Dual-Use Technology', *Defence and Peace Economics*, 35(2), pp. 192–205; https://doi.org/10.1080/10242694.2022.2145645.

Bown, C.P. (2020) 'Export Controls: America's Other National Security Threat', *Duke Journal of Comparative & International Law*, 30(2), pp. 283–308, Available at: https://scholarship.law.duke.edu/djcil/vol30/iss2/4 (Accessed: 17 March 2024).

Bown, C.P. (2023) 'The Challenge of Export Controls', *Finance & Development*, 60(2), pp. 18–21.

Brandt, L. (1994) 'Defense Conversion and Dual-Use Technology', *Policy Studies Journal*, 22(2), pp. 359–370; https://doi.org/10.1111/j.1541-0072.1994.tb01474.x.

Bräuner, O. (2013) 'Beyond the Arms Embargo: EU Transfers of Defense and Dual-Use Technologies to China', *Journal of East Asian Studies*, 13(3), pp. 457–482; https://doi.org/10.1017/S1598240800008304.

Bremer-Maerli, M., Johnston, R.G. (2002) 'Safeguarding This and Verifying That: Fuzzy Concepts, Confusing Terminology, and Their Detrimental Effects on Nuclear Husbandry', *The Nonproliferation Review*, 9(1) pp. 54–82; https://doi.org/10.1080/10736700208436874.

van der Bruggen, K. (2012) 'Possibilities, Intentions and Threats: Dual Use in the Life Sciences Reconsidered', *Science and Engineering Ethics*, 18(4), pp. 741–56; https://doi.org/10.1007/s11948-011-9266-2.

Brunk, G.G., Jason, G.J. (1981) 'The impact of warfare on the rate of invention: A time series analysis of United States patent activity', *Scientometrics*, 3(6), pp. 437–455; https://doi.org/10.1007/BF02017436.

Bureau of Industry and Security (2022) 'Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)', 17 October. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file (Accessed: 15 December 2023).

Bureau of Industry and Security (2023a) 'Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern', 17 October. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file (Accessed: 15 December 2023).

Bureau of Industry and Security (2023b) 'Supplement No. 1 to Part 774, Title 15. Category 1', 8 December. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2332-category-1-materials-chemicals-microorganisms-and-toxins-4/file (Accessed: 30 January 2024).

Bureau of Industry and Security (2024a) 'Supplement No. 1 to Part 774, Title 15. Category 4', 13 March. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2335-ccl4-5/file (Accessed: 30 March 2024).

Bureau of Industry and Security (2024b) 'Supplement No. 1 to Part 774, Title 15. Category 5 Part 1', 17 November. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2337-ccl5-pt2-4/file (Accessed: 30 March 2024).

Bureau of Industry and Security (2024c) 'Supplement No. 1 to Part 774, Title 15. Category 5 Part 2', 13 March. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2336-ccl5-pt1-3/file (Accessed: 30 March 2024).

Buzan, B., Wæver, O. (2009) 'Macrosecuritisation and security constellations: reconsidering scale in securitisation theory', *Review of International Studies*, 35(2), pp. 253–276; https://doi.org/10.1017/S0260210509008511.

Bzhilianskaya, L.Y. (1996) 'Civil applications of dual-use technology in Russia' in Mitcham, C. et al. (eds.) *1996 International Symposium on Technology and Society: Technical Expertise and Public Decisions. Proceedings*. Princetown, New Jersey: IEEE, pp. 25–34; https://doi.org/10.1109/istas.1996.540423.

Campbell, P. (2006) 'Empowerment and restraint in scientific communication: New developments make it easier to share information, but more difficult to deal with dual-use biology', *EMBO Reports*, 7(SI), pp. S18–22; https://doi.org/10.1038/sj.embor.7400710.

Chemical Weapons Convention (1993) Paris, New York, NY, 13 January 1993. [Online]. Available at: https://www.opcw.org/chemical-weapons-convention (Accessed: 5 November 2023).

Chorzempa, M., von Daniels, L. (2023) 'New US Export Controls: Key Policy Choices for Europe', *SWP Comment*, 2023/C 20, 24 March 2023, *Stiftung Wissenschaft und Politik*; https://doi.org/10.18449/2023C20.

Christie, Ø.S., Jakobsen, J., Jakobsen, T.G. (2024) 'The US Way or Huawei? An Analysis of the Positioning of Secondary States in the US-China Rivalry', *Journal of Chinese Political Science*, 29(1), pp. 77–108; https://doi.org/10.1007/s11366-023-09858-y.

Chu, M.-C.M. (2008) 'Controlling the Uncontrollable: The Migration of the Taiwanese Semiconductor Industry to China and Its Security Ramifications', *China Perspectives*, 2008/1, pp. 54–68; https://doi.org/10.4000/chinaperspectives.3343.

Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology (2004*) Biotechnology Research in an Age of Terorism*. Washington, DC: The National Academies Press. [Online]. Available at: https://nap.nationalacademies.org/catalog/10827/biotechnology-research-in-an-age-of-terrorism (Accessed: 25 October 2023).

Congressional Research Service (2020) 'The U.S. Export Control System and the Export Control Reform Initiative' R41916, 28 January. [Online]. Available at: https://sgp.fas.org/crs/natsec/R41916.pdf (Accessed: 20 November 2023).

Congressional Research Service (2021) 'The U.S. Export Control System and the Export Control Reform Act of 2018' R46814, 7 June. [Online]. Available at: https://crsreports.congress.gov/product/pdf/R/R46814 (Accessed: 20 November 2023).

Cook, R.J., Ohle, M., Han, Z. (2022) 'The Illusion of the China-US-Europe Strategic Triangle: Reactions from Germany and the UK', *Journal of Chinese Political Science*, 27(3), pp. 493–518; https://doi.org/10.1007/s11366-021-09771-2.

Czarkowski, M. (2010) 'The Dilemma of Dual Use Biological Research: Polish Perspective', *Science and Engineering Ethics*, 16(1), pp. 99–110; https://doi.org/10.1007/s11948-008-9078-1.

Davis, I. (2002) *The Regulation of Arms and Dual-Use Exports. Germany, Sweden and the UK*. Oxford: SIPRI – Oxford University Press. Available at: https://www.sipri.org/sites/default/files/files/books/SIPRI02Davis.pdf (Accessed: 27 October 2023).

Deng, Y. (2020) 'The Role of the EU in Asian Security: Between Transatlantic Coordination and Strategic Autonomy', *Asia Policy*, 15(1), pp. 105–126; https://doi.org/10.1353/asp.2020.0001.

Dubov, A. (2014) 'The concept of governance in dual-use research', *Medicine, Health Care and Philosophy*, 17(3), pp. 447–457; https://doi.org/10.1007/s11019-013-9542-9.

Dumbacher, E.D. (2018) 'Limiting cyberwarfare: applying arms-control models to an emerging technology', *The Nonproliferation Review*, 25(3–4), pp. 203–222; https://doi.org/10.1080/10736700.2018.1515152.

Erbay, C. (2023) T*he Third Biotechnology Revolution: Synthetic Biology and its Regulation in the European Union*. Tilburg: Tilburg University. [Online]. Available at: https://arno.uvt.nl/show.cgi?fid=162927 (Accessed: 30 September 2023).

European Commission (2023) 'Compilation of national control lists under Article 9(4) of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, PUB/2023/1267' OJ C C2023/441, 20 October. [Online]. Available at: https://eur-lex.europa.eu/eli/C/2023/441/oj (Accessed: 20 December 2023).

European Commission (2024a) *Exporting dual-use items*. [Online]. Available at: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en (Accessed: 15 February 2024).

European Commission (2024b) 'White Paper on Export Controls' COM(2024) 25 final, 24 January. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025 (Accessed: 1 March 2024).

European Commission, Directorate-General for Communications Networks, Content and Technology (2024) 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Analysis of the final compromise text with a view to agreement'. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf (Accessed: 25 February 2024).

Evans, S.W. (2022) 'When All Research Is Dual Use', *Issues in Science and Technology*, 38(3), pp. 84–87.

Export Authorization Regulations (EAR) (2024) *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear (Accessed: 19 February 2024).

Export Control Reform Act of 2018 (2018) U.S. Congress, 15 February 2018. [Online]. Available at: https://www.congress.gov/bill/115th-congress/house-bill/5040/text (Accessed: 19 September 2023).

Fägersten, B., Lovcalic, U., Regnér, A.L., Vashishtha, S. (2023) 'Controlling critical technology in an age of geoeconomics: Actors, tools, and scenarios', *The Swedish Institute of International Affairs*, 2023/1. [Online]. Available at: https://www.ui.se/globalassets/butiken/ui-report/2023/ui-report-no.1-2023.pdf (Accessed: 18 February 2024).

Floyd, R. (2007) 'Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies', *Review of International Studies*, 33(2), pp. 327–350; https://doi.org/10.1017/S026021050700753X.

Flynn, C. (2020) 'Recommendations on Export Controls for Artificial Intelligence', *Center for Security and Emerging Technology Issue Brief*, February 2020. [Online]. Available at: https://cset.georgetown.edu/publication/recommendations-on-export-controls-for-artificial-intelligence/ (Accessed: 18 February 2024).

Forge, J. (2010) 'A Note on the Definition of "Dual Use"', *Science and Engineering Ethics*, 16(1), pp. 111–118; https://doi.org/10.1007/s11948-009-9159-9.

Fox, J.L. (2004) 'US to safeguard "dual-use" biology research', *Nature Biotechnology*, 369(22); https://doi.org/10.1038/nbt0404-369.

Fuhrmann, M. (2008) 'Exporting Mass Destruction? The Determinants of Dual-Use Trade', *Journal of Peace Research*, 45(5), pp. 633–652; https://doi.org/10.1177/0022343308094324.

Gearon, L. (2017) 'The counter-terrorist campus: Securitisation theory and university securitisation – Three Models', *Transformation in Higher Education*, 2(a13); https://doi.org/10.4102/the.v2i0.13.

Gearon, L., Parsons, S. (2019) 'Research Ethics in the Securitised University', *Journal of Academic Ethics*, 17(1), pp. 73–93; https://doi.org/10.1007/s10805-018-9317-2.

Gehrke, T., Ringhof, J. (2023a) 'Caught in the crossfire: Why EU states should discuss strategic export controls', *European Council on Foreign Relations* [Preprint], 11 January 2023. [Online]. Available at: https://ecfr.eu/article/caught-in-the-crossfire-why-eu-states-should-discuss-strategic-export-controls/ (Accessed: 24 November 2023).

Gehrke, T., Ringhof, J. (2023b) 'The power of control: How the EU can shape the new era of strategic export restrictions', *European Council on Foreign Relations*, 17 May 2023. [Online]. Available at: https://ecfr.eu/publication/the-power-of-control-how-the-eu-can-shape-the-new-era-of-strategic-export-restrictions/ (Accessed: 24 November 2023).

Gewirtz, P. (1996) 'On "I Know It When I See It"', *The Yale Law Journal*, 105(4), pp. 1023–1047; https://doi.org/10.2307/797245.

Grahame, D., Mendelsohn, J. (eds.) (2002) *Arms Control Chronology*. Washington, DC: The Center for Defense Information.

Griffiths, P. (2019) 'Updates from the Wassenaar Arrangement', *SMi FourteenthAnnual Conference Defence Exports*, pp. 1–8.

Herr, T., Rosenzweig, P. (2016) 'Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model', *Journal of National Security Law & Policy*, 8(2), pp. 301–319.

Herrmann, C. (2023) 'Open Strategic Autonomy – New challenges for the EU's Common Commercial Policy' *SIEPS – Swedish Institute for European Policy Studies*, June 2023. [Online]. Available at: https://www.sieps.se/globalassets/publikationer/2023/2023_9epa.pdf (Accessed: 9 September 2023).

Himmelfreundpointner, R. (2017) 'Le Monde Wassenaar Arrangement', *Cercle Diplomatique*, 2017/1, pp. 62–66.

Hofhansel, C. (1993) 'From containment of communism to Saddam: The evolution of export control regimes', *Arms Control*, 14(3), pp. 371–404; https://doi.org/10.1080/01440389308404046.

Hrynkiv, O. (2022) 'Export Controls and Securitization of Economic Policy: Comparative Analysis of the Practice of the United States, the European Union, China, and Russia', *Journal of World Trade*, 56(4), pp. 633–656; https://doi.org/10.54648/trad2022026.

Independent High-Level Expert Group on Artificial Intelligence (2019a) 'A Definition of AI: Main Capabilities and Disciplines' *Brussels: European Commission*, 8 April. [Online]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651 (Accessed: 5 April 2023).

Independent High-Level Expert Group on Artificial Intelligence (2019b) 'Ethics Guidelines for Trustworthy AI' *Brussels: European Commission*, 8 April. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Accessed: 5 April 2023).

Independent High-Level Expert Group on Artificial Intelligence (2020a) 'Assessment List for Trustworthy Artificial Intelligence' *Brussels: European Commission*, 17 July. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (Accessed: 5 April 2023).

Independent High-Level Expert Group on Artificial Intelligence (2020b) 'Sectoral Considerations on the Policy and Investment Recommendations for Trustworthy Artificial Intelligence' *Brussels: European Commission*. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (Accessed: 5 April 2023).

Industry and Security Bureau (2018) 'Review of Controls for Certain Emerging Technologies', 19 November. [Online]. Available at: https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies (Accessed: 15 November 2023).

Johnson, W.G. (2019) 'Governance Tools for the Second Quantum Revolution', *Jurimetrics*, 59(4), pp. 487–521.

Kanetake, M. (2019) 'The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches', *Business and Human Rights Journal*, 4(1), pp. 155–162; https://doi.org/10.1017/bhj.2018.18.

Katz, J.I. (2020) 'Education and Training as a Disruptive Dual Use Technology' in Martellini, M., Trapp, R. (eds.) *21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies*. 1st edn. Cham: Springer International Publishing, pp. 205–210; https://doi.org/10.1007/978-3-030-28285-1_10.

Kelsen, H. (1991) 'Legal Norms and Legal Principles: Esser's Transformation Theory' in Kelsen, H., Hartney, M. (eds.) *General Theory of Norms*. online edn. Oxford: Oxford Academic, pp. 115–122; https://doi.org/10.1093/acprof:oso/9780198252177.003.0028.

Kim, H. (2021) 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue', *The International and Comparative Law Quarterly*, 70(2), pp. 379–415; https://doi.org/10.1017/S0020589321000105.

Klaus, M.D. (2003) 'Dual-Use Free Trade Agreements: The Contemporary Alternative to High-Tech Export Controls', *Denver Journal of International Law & Policy*, 32(1), pp. 105–134.

Köstner, D., Nonn, M. (2023) 'The 2020 Chinese export control law: a new compliance nightmare on the foreign trade law horizon?', *China-EU Law Journal*, 8(3), pp. 81–95; https://doi.org/10.1007/s12689-021-00092-4.

Krolikowski, A., Hall, T.H. (2023) 'Non-decision decisions in the Huawei 5G dilemma: Policy in Japan, the UK, and Germany', *Japanese Journal of Political Science*, 24(2), pp. 171–189; https://doi.org/10.1017/S146810992200038X.

Lazarou, E., Lokker, N. (2019) *United States: Export Control Reform Act (ECRA)*. European Parliamentary Research Service. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/644187/EPRS_BRI(2019)644187_EN.pdf (Accessed: 13 December 2023).

Legrand, J. (1999) 'Some guidelines for fuzzy sets application in legal reasoning', *Artificial Intelligence and Law*, 7(2), pp. 235–257; https://doi.org/10.1023/A:1008357323873.

Lupovici, A. (2021) 'The dual-use security dilemma and the social construction of insecurity', *Contemporary Security Policy*, 42(3), pp. 257–285; https://doi.org/10.1080/13523260.2020.1866845.

Mahfoud, T., Aicari, C., Datta, S., Rose, N. (2018) 'The Limits of Dual Use', *Issues in Science and Technology*, 34(4), pp. 73–78.

Martins, B.O., Küsters, C. (2019) 'Hidden Security: EU Public Research Funds and the Development of European Drones', *JCMS: Journal of Common Market Studies*, 57(2), pp. 278–297; https://doi.org/10.1111/jcms.12787.

Maurer, S.M., Fischer, M. (2010) 'How to Control Dual-Use Technologies in the Age of Global Commerce', *Bulletin of the Atomic Scientists*, 66(1), pp. 41–47; https://doi.org/10.2968/066001006.

McCormick, D. (2006) 'Exports to China must not be used to develop the military [Asia Edition]', *Financial Times*, p. 13.

Meng, J.-H., Wang, J. (2023) 'The policy trajectory of dual-use technology integration governance in China: A sequential analysis of policy evolution', *Technology in Society*, 2023/72, p. 102175; https://doi.org/10.1016/j.techsoc.2022.102175.

Miller, S. (2018) 'Concept of Dual Use' in Miller, S. (ed.) *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Cham: Springer International Publishing, pp. 5–20; https://doi.org/10.1007/978-3-319-92606-3_2.

Mir, T.u.G., Wani, A.K., Akhtar, N., Shukla, S. (2022) 'CRISPR/Cas9: Regulations and challenges for law enforcement to combat its dual-use', *Forensic Science International*, 2022/334, 111274; https://doi.org/10.1016/j.forsciint.2022.111274.

Moore, G.J. (2023) 'Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies', *Journal of Chinese Political Science*, 28(1), pp. 151–167; https://doi.org/10.1007/s11366-022-09814-2.

Pillar, P.R. (2023) 'Export Controls and the Junction of Economics and National Security: A Review Article', *Political Science Quarterly*, qqad075; https://doi.org/10.1093/psquar/qqad075.

Puranik, T.G. (2021) 'The Impacts of Proliferation and Autonomy of Small Unmanned Aircraft Systems on Security' in Kosal, M.E. (ed.) *Proliferation of Weapons- and Dual-Use Technologies: Diplomatic, Information, Military, and Economic Approaches*. Cham: Springer International Publishing, pp. 33–52. [Online]. Available at: https://doi.org/10.1007/978-3-030-73655-2_4.

Pustovit, S.V., Williams, E.D. (2010) 'Philosophical Aspects of Dual Use Technologies', *Science and Engineering Ethics*, 16(1), pp. 17–31; https://doi.org/10.1007/s11948-008-9086-1.

Qi, Y., Chu, X. (2022) 'Development of the digital economy, transformation of the economic structure and leaping of the middle-income trap', *China Political Economy*, 5(1), pp. 14–39; https://doi.org/10.1108/CPE-09-2022-0012.

Rager-Zisman, B. (2012) 'Ethical and Regulatory Challenges Posed by Synthetic Biology', *Perspectives in Biology and Medicine*, 55(4), pp. 590–607; https://doi.org/10.1353/pbm.2012.0043.

Raivo, R., Trišč uka, J. (2023) 'The EU's control list of dual-use items has been updated', *Sorainen*, 27 February 2023. [Online]. Available at: https://www.sorainen.com/publications/the-eu-s-control-list-of-dual-use-items-has-been-updated/ (Accessed: 15 November 2023).

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), pp. 769–790; https://doi.org/10.1007/s11948-014-9519-y.

Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (consolidated text) (2019) OJ L 079I, 21 March 2019. [Online]. Available at: http://data.europa.eu/eli/reg/2019/452/2021-12-23 (Accessed: 29 November 2023).

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (2021) OJ L 206, 11 June 2021. [Online]. Available at: https://eur-lex.europa.eu/eli/reg/2021/821/oj (Accessed: 19 September 2023).

Reinsch, W.A., Schleich, M., Denamiel, T. (2023) 'Insight into the U.S. Semiconductor Export Controls Update', *Center for Strategic & International Studies*, 20 October 2023. [Online]. Available at: https://www.csis.org/analysis/insight-us-semiconductor-export-controls-update (Accessed: 30 December 2023).

Ruohonen, J., Kimppa, K.K. (2019) 'Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity', *Journal of Information Technology & Politics*, 16(2), pp. 169–186; https://doi.org/10.1080/19331681.2019.1616646.

Rychnovská, D. (2016) 'Governing dual-use knowledge', *Security Dialogue*, 47(4), pp. 310–328; https://doi.org/10.1177/0967010616658848.

Sánchez-Cobaleda, A. (2022) 'Defining "dual-use items": legal approximations to an ever-relevant notion', *The Nonproliferation Review*, 29(1–3), pp. 77–95; https://doi.org/10.1080/10736700.2023.2202966.

Sarah, M., Andreas, R., Hakan, E. (2023) 'German proposal for Huawei curbs triggers telecom operator backlash', *Reuters* [Preprint], 20 September 2023. [Online]. Available at: https://www.reuters.com/business/media-telecom/german-interior-ministry-wants-force-5g-operators-slash-huawei-use-official-2023-09-19/ (Accessed: 30 October 2023).

Schmid, S., Riebe, T., Reuter, C. (2022) 'Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D', *Science and Engineering Ethics*, 28(2); https://doi.org/10.1007/s11948-022-00364-7.

Schneider, J., Meske, C., Kuss, P. (2024) 'Foundation Models', *Business & Information Systems Engineering*; https://doi.org/10.1007/s12599-024-00851-0.

Selgelid, M.J. (2009) 'Dual-Use Research Codes of Conduct: Lessons from the Life Sciences', *NanoEthics*, 3(3), pp. 175–183; https://doi.org/10.1007/s11569-009-0074-y.

Selgelid, M.J. (2013) 'Biodefense and dual-use research: the optimisation problem and the value of security', *Journal of Medical Ethics*, 39(4), p. 205; https://doi.org/10.1136/medethics-2012-100923.

Seyoum, B. (2017) 'National Security Export Control Regimes: Determinants and Effects on International Business', *Thunderbird International Business Review*, 59(6), pp. 693–708. [Online]. Available at: https://doi.org/10.1002/tie.21819.

Shagina, M. (2023) 'The Role of Export Controls in Managing Emerging Technology' in Berghofer, J. et al. (eds.) *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network*. Cham: Springer International Publishing, pp. 57–72; https://doi.org/10.1007/978-3-031-24673-9_4.

Skolnikoff, E.B. (2008) 'Responding to asymmetric threat: The dual-use strategy', *Dynamics of Asymmetric Conflict*, 1(1), pp. 42–47; https://doi.org/10.1080/17467580802054545.

Stone, M. (2012) 'Global Regulations for Dual-Use Research Tighten', *Bioscience*, 62(6), p. 616; https://doi.org/10.1525/bio.2012.62.6.17.

Stritzel, H. (2007) 'Towards a Theory of Securitization: Copenhagen and Beyond', *European Journal of International Relations*, 13(3), pp. 357–383; https://doi.org/10.1177/1354066107080128.

Taureck, R. (2006) 'Securitization theory and securitization studies', *Journal of International Relations and Development*, 9(1), pp. 53–61; https://doi.org/10.1057/palgrave.jird.1800072.

The State Council of China (2021) 'China's Export Controls' Xinhua, 29 December. [Online]. Available at: https://english.www.gov.cn/archive/whitepaper/202112/29/content_WS61cc01b8c6d09c94e48a2df0.html (Accessed: 15 December 2023).

The Wassenaar Arrangement Secretariat (2023) 'List of Dual-Use Goods and Technologies and Munitions List' *WA-List (23)1*, 1 December. [Online]. Available at: https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf (Accessed: 29 February 2024).

The White House (2023) *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 October 2023. [Online]. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (Accessed: 10 December 2023).

Thompson, K. (2024) 'How the Drone War in Ukraine Is Transforming Conflict, Council on Foreign Relations', *Council on Foreign Relations*, 16 January 2024. [Online]. Available at: https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict (Accessed: 11 February 2024).

Tongele, T.N. (2022a) 'Emerging & Foundational Technology Controls: A General Overview', *BIS 2022. Update Conference on Export Controls and Policy*, 29 June 2022. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file (Accessed: 30 November 2023).

Tongele, T.N. (2022b) 'Emerging and Foundational Technology Controls', *AUECO – Export Controls and Research Security at Higher Education and Scientific Institutions*, 4 May 2022. [Online]. Available at: https://researchservices.upenn.edu/wp-content/uploads/2022/04/Emerging-and-Foundational-tech.pdf (Accessed: 30 November 2023).

Treaty on the Non-Proliferation of Nuclear Weapons (1968) Moscow, Russia, London, Washington, DC, 1 July 1968. [Online]. Available at: https://disarmament.unoda.org/wmd/nuclear/npt/ (Accessed: 15 November 2023).

UNODA (1972) *The Biological Weapons Convention*. [Online]. Available at: https://disarmament.unoda.org/biological-weapons/ (Accessed: 12 November 2023).

UNODA (2004) *UN Security Council Resolution 1540 (2004)*. [Online]. Available at: https://disarmament.unoda.org/wmd/sc1540/ (Accessed: 13 November 2023).

Urbina, F., Lentzos, F., Invernizzi, F., Ekins, S. (2022) 'A teachable moment for dual-use', *Nature Machine Intelligence*, 4(7), pp. 607–607; https://doi.org/10.1038/s42256-022-00511-6.

Vandenberghe, K. (2021) 'Dual-Use Regulation 2021/821: What's Old & What's New in EU Export Control', *Global Trade and Customs Journal*, 16(9) pp. 479–488; https://doi.org/10.54648/gtcj2021053.

Voetelink, J. (2022) 'International Export Control Law – Mapping the Field' in Beeres, R., Bertrand, R., Klomp, J., Timmermans, J., Voetelink, J. (eds.) *NL ARMS Netherlands Annual Review of Military Studies 2021: Compliance and Integrity in International Military Trade*. 1st edn. The Hague: T.M.C. Asser Press, pp. 69–94; https://doi.org/10.1007/978-94-6265-471-6_5.

The Wassenaar Arrangement Secretariat (2023) 'List of Dual-Use Goods and Technologies and Munitions List' *WA-List (23)1*, 1 December. [Online]. Available at: https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf (Accessed: 29 February 2024).

Weinberger, S. (2009) 'Export-control laws worry academics', *Nature*, 461(7261), p. 156; https://doi.org/10.1038/461156a.

Whang, C. (2021) 'Trade and Emerging Technologies: A Comparative Analysis of the United States and the European Union Dual-Use Export Control Regulations', *Security and Human Rights*, 31(1–4), pp. 11–34; https://doi.org/10.1163/18750230-31010007.

The White House (2023) *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. 30 October 2023. [Online]. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (Accessed: 10 December 2023).

World Economic Forum: Centre for the Fourth Industrial Revolution (2023) 'Top 10 Emerging Technologies of 2023' *Geneva: World Economic Forum*, 26 June. [Online]. Available at: https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2023.pdf (Accessed: 25 October 2023).

Yoo, C.S., Mueller, A. (2024) 'Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena', *Federal Communications Law Journal*, 76(2), pp. 143–215.

Yoshizawa, G., Shinomiya, N., Kawamoto, S., Kawahara, N., Kiga, D., Hanaki, K.I., Minari, J. (2023) 'Limiting open science? Three approaches to bottom-up governance of dual-use research of concern', *Pathogens and Global Health*, 118(4), pp. 285–294; https://doi.org/10.1080/20477724.2023.2265626.

Zwartkruis, W. (2024) 'Foreign Direct Investment and Security: What is Actually the Problem?' in Hillebrand-Pohl, J., Papadopoulos, T., Wiesenthal, J. (eds.) *National Security and Investment Controls*. 1st edn. Cham: Springer Nature Switzerland, pp. 1–32; https://doi.org/10.1007/17280_2024_29.

Chopping the Red Tape (1998) *Business Europe*, 38(17), pp. 4–5.

Deemed exports (no date) *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.gov/deemed-exports (Accessed: 25 January 2024).

Deemed Exports and Fundamental Research for Biological Items (2024) *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/chemical-and-biological-controls/14-policy-guidance/deemed-exports/111-deemed-export-and-fundamental-research-for-biological-items (Accessed: 30 January 2024).

Final Document of the BWC Sixth Review Conference (2006). [Online]. Available at: https://bwc1972.org/publication/final-document-of-the-bwc-sixth-review-conference-2006/ (Accessed: 15 September 2023).

The International Traffic in Arms Regulation (ITAR) (2024) *Directorate of Defense Trade Controls*. [Online]. Available at: https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987 (Accessed: 19 February 2024).

Missile Technology Control Regime Guidelines (2023) *MTCR*. [Online]. Available at: https://www.mtcr.info/en/mtcr-guidelines (Accessed: 10 December 2023).

Nuclear Suppliers Group Guidelines (no date) *Nuclear Suppliers Group*. [Online]. Available at: https://www.nuclearsuppliersgroup.org/index.php/en/guidelines/nsg-guidelines (Accessed: 15 November 2023).

Officials Show Scant Interest in Major Export Control Overhaul for China (2011) *Inside US Trade*, 29(38). [Online]. Available at: https://www.proquest.com/trade-journals/officials-show-scant-interest-major-export/docview/913046784/se-2 (Accessed: 29 September 2023).

Supplement No. 4 to Part 744, Title 15. Entity List (2024) *Code of Federal Regulations*. [Online]. Available at: https://www.ecfr.gov/current/title-15/part-744/appendix-Supplement No. 4 to Part 744 (Accessed: 21 March 2024).

The United States Announces Export Controls to Restrict China's Ability to Purchase and Manufacture High-End Chips (2023) *The American Journal of International Law*, 117(1), pp. 144–150; https://doi.org/10.1017/ajil.2022.89.

United States: Proposed Changes to the EU Dual-Use Export Control Regime (2016) *MENA Report*. [Online]. Available at: https://www.proquest.com/wire-feeds/united-states-proposed-changes-eu-dual-use-export/docview/1824526908/se-2 (Accessed: 15 September 2023).

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995). [Online]. Available at: https://www.wassenaar.org/ (Accessed: 25 November 2023).