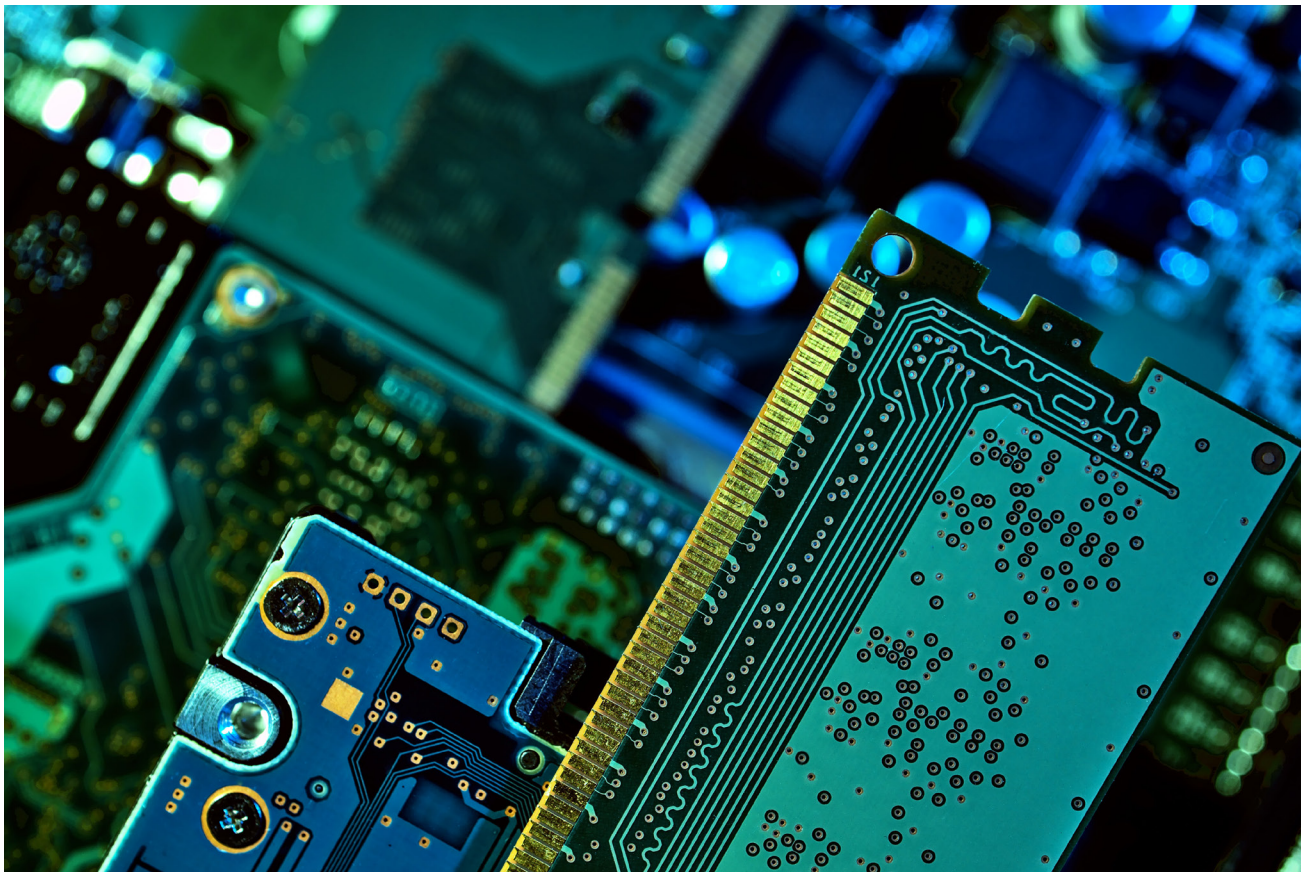
PRIO

Independent • International • Interdisciplinary

PRIO PAPER 2022

Dual-Use AI Technology in China, the US and the EU

Strategic Implications for the Balance of Power



Ilaria Carrozza
Peace Research Institute Oslo (PRIO)

Nicholas Marsh
Peace Research Institute Oslo (PRIO)

Gregory M. Reichberg
Peace Research Institute Oslo (PRIO)

Peace Research Institute Oslo (PRIO)
PO Box 9229 Grønland, NO-0134 Oslo, Norway
Visiting Address: Hausmanns gate 3

www.prio.org
Facebook: PRIO.org
Twitter: PRIOresearch

ISBN: 978-82-343-0367-8 (print)
978-82-343-0368-5 (online)

Cover photo: Michael Dziedzic / Unsplash

Dual-Use AI Technology in China, the US and the EU

Strategic Implications for the Balance of Power

Ilaria Carrozza
Peace Research Institute Oslo (PRIO)

Nicholas Marsh
Peace Research Institute Oslo (PRIO)

Gregory M. Reichberg
Peace Research Institute Oslo (PRIO)

Peace Research Institute Oslo (PRIO)
Hausmanns gate 3
PO Box 9229 Oslo
NO-0134 Oslo, Norway
Tel. +47 22 54 77 00
www.prio.org

PRIO encourages its researchers and research affiliates to publish their work in peer-reviewed journals and book series, as well as in PRIO's own Paper and Policy Brief series. In editing these series, we undertake a basic quality control, but PRIO does not as such have any view on political issues. We encourage our researchers actively to take part in public debates and give them full freedom of opinion. The responsibility and credit for the hypotheses, theories, findings and views expressed in our publications thus rest with the authors themselves.



This work is licensed under CC BY 4.0. The contents can be shared and processed for free, provided that the author is credited correctly, indicating whether changes have been made, and without suggesting that the licensor endorses the use of the work.

ISBN: 978-82-343-0367-8 (print)
ISBN: 978-82-343-0368-5 (online)

Cover design: www.medicineheads.com
Cover photo: Michael Dziedzic / Unsplash

Contents

Funding 6
Executive Summary 7
Introduction 10
Methodology 12
1. Defining AI and "Dual-Use" Technology 13
2. Developing and Regulating Dual-Use AI Technology: China, the US and the EU 19
2.1. China 20
2.2. The US 23
2.3. The EU 27
3. Strategic Implications for the Balance of Power 30
Conclusion and Recommendations for Norway 33
Notes 35
Bibliography 43

Funding

Research for this report was funded by the Norwegian Ministry of Defence.

Executive Summary

Recent policy documents on artificial intelligence (AI) have voiced a concern that **emerging, AI-enhanced technologies have the potential to radically shift the military balance of power worldwide**. Vladimir Putin put the point dramatically when he said in 2017 that "whoever becomes the leader of [AI research] will become the ruler of the world." However, despite the Ukraine conflict (where Russia has exhibited few advanced AI capabilities), it is China that remains the main locus of Western concern.

Over the last ten years, **China has achieved undeniable success in AI research and development**. Some experts now identify a growing edge in China's work on AI military applications vis-à-vis American efforts. Alarm about China's imminent pre-eminence may be inflated, but there is worry that normative considerations constrain Chinese military AI applications differently than they do in the United States and Europe. Moreover, China has a burgeoning civilian AI sector that functions in close synergy with the military sector; indeed, China's official policy of **"military-civil fusion"** is thought to give the country an advantage over the United States and Europe, as the latter societies operate under the principle that the two spheres should be kept separate in the measure possible, with controls placed on the transference of technology from the one to the other. Further, many civilian AI engineers in the West are averse to working on military projects, a reluctance that is perceived to work in China's interest.

Unlike military transformations of the past, where innovation often emerged from within the military-industrial complex, **today the civilian IT sector stands at the forefront of technological change**. Militaries across the globe are racing to keep up with the cycles of innovation. They harbor a constant worry that disruptive technologies will render time-honored strategies obsolete, hence the race to apply and integrate AI technologies within military planning at a faster rate than one's competitors and adversaries. Because the crucial drivers of this process are civilian technologies—hardware and software—the question of **how to retain control over commercial products, so they cannot be put to adversarial military use**, looms high on the policy agenda for government officials who are tasked with defense and foreign affairs.

"Dual-use technology"—long a mainstay of discussions about nuclear technology—has taken on a whole new meaning and urgency in the context of AI-enhanced warfare. Whereas nuclear weapons are difficult to build and transport without detection, the new digital technologies are made from algorithmic lines of code, which are easily transferred across borders. Making use of these codes does rely on physical infrastructure, hence the growing pressure to restrict flows of strategically important technologies such as the most advanced computers, chip design tools and the like. As these technologies are intimately emmeshed within the civilian communications and IT sectors and are fundamental to the free flow of goods and services across the globe, placing restrictions on the broad array of items that can be classed as "dual use" raises challenging questions that this report aims to address.

This report acknowledges that the key terms "AI" and "dual use" are notoriously difficult to define. With respect to **AI**, we focus on **algorithmic functions performed by a computer** that (i) *enhance* human decision-making through input from sensors and large data pools (human in the loop) or (ii) increase the speed of decisions by *automating* the decision process, whereby selection of options is delegated to a machine operating autonomously, but ideally under human supervision (human on the loop). AI technology comprises both hardware and software. AI systems will comprise several components that are not in themselves defined as AI. For example, a microchip is essential for running AI software, but on its own the chip is not an example of AI and may have many non-AI uses. An AI system may well comprise several different elements which only constitute artificial intelligence when they are combined.

With respect to **"dual use,"** we observe that, beyond its **common-sense meaning of "items which can have both civil and military uses,"** there exists no internationally agreed definition of what constitutes a weapon or military equipment, nor, apart from lists of dual-use items, do we find "dual use" defined as a general term. From the standpoint of the regulator, the lack of conceptualized, overarching definitions is a pragmatic choice. These items are regulated via long lists of controlled goods which can be edited to add or remove new items without the need to consider, for example, whether new technology meets pre-existing criteria.

Classifying and identifying AI as a dual-use technology poses profound challenges for regulators in China, the European Union (EU) and the United States (US). In the past, controlled goods were usually physical objects whose trade could be monitored by customs officers stationed at ports. Dual-use AI technology poses special problems for trade controls as key aspects of the technology are based upon software.

While many countries are currently pursuing research in dual-use AI technology, we focus on China, the US and the EU because the former two have emerged as the main actors in developing this technology, while the latter is attempting to dominate global efforts to regulate dual-use AI. These developments are happening against the background of an ongoing competition for technology dominance, which will have significant effects on the future balance of military power.

China intends to leverage AI as part of its **plans to build highly technological weapons that would seriously challenge US armed forces** (especially in the Indo-Pacific). Commercial advancements in dual-use technology have been beneficial to the defense sector and, according to some, these advancements will allow China to conduct AI warfare in such a way as to ensure battlefield "brain supremacy." Alongside efforts to boost China as a leader in developing and producing new technologies, the government is striving to regulate the field. The 2020 Export Control Law restricts exports of military and dual-use products and technology for national security and public policy reasons. Specific technological areas included are: unmanned aerial vehicles (UAVs);

information processing technologies—for instance, personal interactive data algorithms; intelligent scoring; and cyber-related technologies.

The **Unites States**' Department of Defense (DoD) has been studying the military potential of AI for well over a decade. In 2018 the DoD launched the **Joint AI Center (JAIC)**, with the aim of establishing a main focal point of AI- related initiatives within the US armed forces. Also in 2018the US government began the regulatory process of introducing new trade controls to prevent actors such as China and Russia from obtaining advanced AI technology developed in the US. Progress has been slow, however, due to the inherent difficulties related to the intangibility of software.

The EU has highlighted AI as a major strategic priority for the near future. Its strategy regarding the development of AI technology has been primarily oriented towards **setting ethical standards** and supporting member states as well as the private sector in complying with such standards and mitigating potential ethical risks. The EU has also taken several steps to increase the coordination and convergence of member states' export controls on dual-use items, for instance by adopting new regulation on export controls of sensitive dual-use technologies in 2021.

The Russian invasion of Ukraine and subsequent EU and US sanctions have the potential to raise the stakes in this rivalry. As well as potential Chinese uses for dual-use AI technology, policymakers in the EU and US also need to consider the risks that China may undermine sanctions by passing on hardware and software to Russia.

AI applications have the potential to shape future conflicts in a number of ways, such as by increasing the speed with which countries can fight. AI systems might also lead to changes in military strategy, for instance by substituting machines for humans in making certain decisions. Furthermore, the perception of any progress in the domain of dual-use technology risks creating a "dual-use security dilemma." **Dual-use technology thus creates yet another layer of uncertainty, as one cannot know whether any given item has been created with civilian or military purposes**.

Within the context of the current Sino-US rivalry, **uncertainties around any progress either country might be making are likely to have implications for the strategic balance of power**. In particular, the pursuit of dual-use AI capabilities in China will continue to fuel the perception in many policy circles within the US and, to a lesser extent, in Europe that the Chinese Communist Party intends to exploit such technology to advance its foreign policy goals, possibly leading to more reactive policies than perhaps is necessary.

Introduction

As the pace of innovations in both the civilian and military domains increases, so do the uncertainties stemming from the use of new technologies. In this report, we focus on dual-use artificial intelligence (AI) technology as a central element in today's great power competition. We understand dual use as referring to items that have both civil and military applications. According to standard nomenclature, AI is a software capability, founded on algorithms and engineered into machines, enabling them (i) to autonomously select among several options in order to achieve goals set by human operators or (ii) to enhance human decision processes by providing rapid input from sensors, big data and large-scale computational resources. In this report, we examine the dual-use technologies that underly AI systems (see Section 1 for more details and definitions).

The dual-use nature of many AI systems is becoming more apparent, as they can be directed to both civilian and military purposes. In particular, many expect that AI technologies will have a transformative impact on military affairs, aiding but also disrupting warfare and society alike.[1] Simultaneously, regulating the export of these technologies is important to policy-making in many nations that are concerned with preventing the proliferation of weapons capable of causing widespread destruction. While AI is a form of software and is not itself a weapon, it enables the formation of weapon systems, for instance those utilized in swarm warfare. In this vein, AI pioneer Stuart Russell warns of the danger that AI technologies could result in "scalable weapons of mass destruction," if thousands of miniature robots, each bearing targetable munitions and endowed with facial-recognition capabilities, are directed against specific individuals or groups.[2] Hence, there is a need to address questions of risk, security and norms posed by the increased use of systems such as facial recognition software, autonomous weapon systems (AWS) and decision-making algorithms.[3]

In this report, we describe current advances in developing dual-use AI technology in China, the EU and the US, and we conclude by considering the strategic implications of these developments for the global balance of power. While there are more countries pursuing research in this field, including Israel and South Korea, we focus on these three as they have emerged as the primary actors behind efforts to either develop or regulate AI.

The Chinese defense establishment has been actively pursuing investments in AI technology and has fostered the transfer of data, software and hardware between its civilian and military sectors in what is called its "military-civil fusion" strategy. At least partly in response to the rapid progress of China's AI efforts, since 2019 the US government has promoted a series of policies, such as the American Artificial Intelligence Initiative, aimed primarily at protecting US leadership in AI technology and restricting flows of data and talent across borders.[4] Indeed, as a result of the current strategic competition, both China and the US are mobilizing enormous resources to build military AI systems, including unmanned attack platforms for swarm warfare and tools enhancing perceptual awareness in battlefield conditions. They are also boosting their domestic

capacity for the innovation and production of advanced dual-use technologies such as semiconductors, surveillance and 5G networking equipment.

In comparison, the EU has generally preferred more of a rule-maker role and is mostly attempting to position itself as a major platform for the international community to address developments in dual-use AI and the ethical concerns raised by their use.[5] However, it too sees the military potential of AI-based systems and has encouraged investing in them.[6]

The consequences of the invasion of Ukraine by Russia reinforce the relevance of this report's findings. NATO members and Russia face levels of mutual antagonism not seen since the end of the Cold War.[7] Sanctions and export restrictions imposed upon Russia by the EU, the US and several other "western" states have, in part, the rationale of preventing Russia from developing high technology weapons. For example, the EU sanctions enacted on the day after the invasion specifically target the export of dual-use software that could be used in military applications.[8] Russia has had a program on the development of military robotics since 2015 and, since 2019, it has had a well-financed national strategy for AI (including its military applications).[9] Russian leaders have generally shown enthusiasm for the "promises" of AI technology, which they view as a tool of information warfare that may compensate for the country's inferiority relative to NATO in terms of conventional weapons.

However, Russia lacks skilled scientists and infrastructure in this field, and thus its development of military AI is dependent upon the import of dual-use AI technology from abroad (particularly advanced semiconductors).[10] Inhibiting the further development of military AI by Russia will require close cooperation between the US and the EU, something which may have political support but whose implementation may be hampered by different regulatory approaches. China will play a key role in the transfer of AI technology to Russia, as its national strategy could either be used to prevent the latter from obtaining dual-use technology, or to undermine EU and US sanctions. Other states that are involved in developing AI, such as Japan or Israel, will similarly have to choose between supporting sanctions directed at Russia or supplying it with dual-use technology.

This report proceeds in three sections. First, we clarify the concepts of "AI", "weapons" and "dual use". Second, we unpack the different Chinese, EU and US policies and strategies on developing and regulating dual-use AI technology, and we discuss some of the challenges that arise from commercial trade in such technologies. Third, we argue that the ensuing strategic competition between the US, the EU and China has implications for the military balance of power. We conclude by making recommendations for how Norway could position itself in the debate over the development of transparent and accountable dual-use AI technology.

Methodology

This report was produced as part of the project "The Role of Dual-Use Artificial Intelligence (AI) Technology in the Current International "Arms" Race", which was funded by the Norwegian Ministry of Defence and studies how dual-use technology can change the geopolitical balance of power.

This report is based on a content analysis of openly available official documents published by the governments and relevant ministries in China and the US, as well as by the European Commission and other relevant organizations (e.g., the European Defence Agency and the Cyberspace Administration of China). Throughout the project, the team has also benefited from informal exchanges with experts in the field of technology and AI across the EU and the US.

During 2021, team members attended high-level meetings convened, inter alia, by the European Defence Agency and the US Naval Academy and have discussed ongoing research in these settings. Preliminary findings of the research were also discussed at a meeting organized in September 2021 by the Norwegian Ministry of Defence.

The report further benefits from synergies with past and ongoing research at the project's host institution, the Peace Research Institute Oslo (PRIO), including projects on the ethics of military AI ('Algor-ethics in the Emerging Battlespace'), on the implementation of AI in military technologies ('Warring with Machines: Military Applications of Artificial Intelligence and the Relevance of Virtue Ethics') and on China's promotion of AI and digital technology in its neighborhood ('Shaping the Digital World Order: Norms and Agency along the Digital Silk Road in Southeast Asia (NORM)').

1. Defining AI and "Dual-Use" Technology

Many in Western military and policy communities are concerned that emerging AI technologies may be used by China for military purposes in the context of the current geostrategic rivalry.[11] The US and the EU have thus been taking steps to impose trade controls over dual-use AI technology (an issue we return to in Section 2), in an attempt to prevent the challenges to peace and cooperation that stem from the proliferation of certain dual-use items. Before looking in detail at those measures, in this section we elaborate on what is meant by "AI", "dual use" and the related concepts of "weapons" and "military equipment."

There is no widely agreed upon definition of artificial intelligence or related concepts such as machine learning (ML). Some common definitions of AI and ML refer to them replicating human intelligence or reasoning. However, these human characteristics are not well defined and comparison to them implicitly rules out novel machine capabilities that may not be found among humans. Here, we adopt the definition suggested by the High-Level Expert Group on Artificial Intelligence set up by the European Commission:

> *Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal.*[12]

This definition is directly relevant to military applications of AI in that it focuses upon the crucial decisions that need to be taken while in combat—in particular the identification of threats and the selection of targets. Additionally, the European Defence Agency (EDA) provides a definition of machine learning that is: "to model systems by learning from the data these systems produce." The key element of this definition is that it can occur without the ongoing intervention of an external programmer as in "unsupervised machine learning."

AI systems can be seen to encompass several different roles in relation to humans. By far the most common contemporary use is human-machine teaming or the augmentation of human intelligence with AI. This use would involve humans making decisions supported by information provided by AI. In a military context, this might involve an AI system warning a pilot of likely threats and possibly recommending a course of action, but leaving the pilot to select the actual target. A second use concerns AI systems that make decisions and act, but which are supervised by a human who can intervene as needed. A civilian example is a self-driving car, which is designed to be used with an alert human driver at the wheel. A third form of AI concerns what are known as "fully autonomous systems," which take decisions and act without direct human intervention. Here, the human operator is neither "in" the decision loop (making the decision based on input from the machine), nor even "on the loop" (supervising the machine with the possibility of intervening), but is strictly speaking "off the loop." Such systems are currently rare, an example being a missile which is

capable of autonomously identifying and selecting a target such as an enemy warship, while avoiding countermeasures and operating in concert with other missiles.[13]

Robots that could operate for long periods in complex environments like a battlefield and are sophisticated enough to distinguish between different contexts such as an irregular enemy soldier or a civilian carrying a weapon for self-protection currently exist only in the realm of science fiction. For this reason, the remainder of this report focuses upon the first two uses (AI augmenting human intelligence, or AI systems that are supervised by humans). Importantly, there is not a clear distinction between the two. For example, a system designed to be one in which AI augments human decision-making by offering recommendations might in practice be a supervised system if the human operator reflexively approved every option presented by the AI (so-called "automation bias").

AI technology comprises both hardware (e.g., mainframe computers and other computational resources, microchips, sensors, effectors and the communication infrastructure that joins together the relevant hardware devices into a seamless whole) and software (e.g., programs and algorithms). In general, AI systems will comprise several components and intangible elements (e.g., algorithms or structured data) that are not in themselves defined as AI.

In this report, we are primarily concerned with dual-use technology that is used to develop, produce and use AI systems. Dual-use equipment is distinct from the weapons used by military forces, and to aid understanding of "dual use" we first explain the terms "weapon" and "military equipment." We define a *weapon* as being *a specialized tool of violence*.[14] Its designers and makers envisage that its primary purpose is to cause non-consensual[15] harm or damage. These terms are defined widely, where harm includes physical injury or mental distress and damage may be caused to living beings, tangible objects (such as buildings) or to the intangible (such as software). The ultimate purpose of a weapon is to multiply human capacity for violence.[16] Most weapons can be used offensively or defensively (i.e., usually there is little point trying to classify a weapon as either). As a tool, a weapon could have a wide variety of forms, including: a physical object or collection of them; an intangible entity (such as a computer virus); or a biological entity (e.g., bacteria designed to be used as a weapon).[17] Some weapons are made up of different units which are physically separate, and collectively, they are known as *a weapon system*. For example, an anti-aircraft system may be made up of integrated missiles, radar and a fire control post, which may be kilometers apart from each other. Each part of the system is necessary for it to function as intended.

Weapons are included in the wider category of *military equipment*. Such equipment is specific to armed forces or security forces and includes items that are not weapons but are used by them in military roles, for example body armor, radar or secure communications.

All but the most basic weapons or pieces of military equipment are made of components.[18] An individual component may not in itself be a useful tool for causing harm or for use by military

forces. For example, a trigger is a vital component of a gun, but on its own a trigger is a harmless piece of metal. Technological innovation in weaponry often occurs when components are combined in novel ways, as for instance when AI software provides miniature drones with computer vision, and these airborne platforms are fitted with recoil-free guns, with the result that a swarm (itself coordinated by multi-agent software enabling communication within the swarm) of such platforms can autonomously select and fire on a set of predetermined targets. As this example shows, the lethality and novelty of the weapon arises not so much from its components taken individually, but from their combination into a particular system.

Dual-use items are those which have both civil and military uses.[19] For example, the EU in its regulation defines dual use as being items "which can be used for both civil and military purposes."[20] Such a definition is potentially very broad. If one thinks hard enough, it is possible to imagine a military use for any item; for example, food or water are essential for the sustainment of all military forces. As is shown below, in practice the term dual use is mainly used to cover items that are used in the development, production or use of weapons or military equipment, but which also have significant civilian uses: for example, a part of a jet engine that could be used in a military or civil aircraft.

There are, unsurprisingly, blurred boundary lines between the different categories of "weapons," "military equipment" and "dual use." Some items can clearly be identified as one or the other (an anti-tank missile is clearly a weapon). But in other cases, it is harder to define particular equipment. For example, in some cases a radar may be an integral part of a weapon (such as in a missile), in other cases radar can be a vital element of a weapon system, and in others a radar may be a stand-alone piece of military equipment. If a radar also has significant civilian uses, it might be categorized as a piece of dual-use equipment.

Despite the existence of multilateral treaties and international organizations concerned with the use of and trade in certain types of weapons, military equipment and dual-use items, and national laws which also cover aspects of their development and production, there exists no internationally agreed definition of what constitutes a weapon or military equipment. Nor have governments or international organizations produced a more in-depth conceptualization of dual-use items.[21]

The ownership, trade, production and use of weapons, military equipment and, to a lesser extent, dual-use goods (see below) are regulated.[22] Overall, this occurs via multi-level governance through international institutions and international law, legislation and regulation, national and local government, traditional or customary authority and societal norms and practices.[23] There is variation in the scope and effectiveness of all these forms of regulation. In all the countries studied, civilian ownership of almost all the weapons used by armed forces is prohibited or tightly regulated, an exception being some types of firearms, particularly in the United States.

The European Union, Norway and the United States have published lengthy lists of controlled goods covering categories of weapons, military equipment and dual-use items.[24] The lists are coordinated internationally by the European Union (for its member states) and the Wassennaar Arrangement, an international organization which works on coordinating export control among its members (which include Norway, major EU arms exporters and the United States, but not China).[25] Due to this coordination, the lists of controlled goods published by the EU and the United States are similar.[26]

China has taken a different approach. While the country has published a long list of controlled goods,[27] it has not published a specific "dual-use" list. Rather, its list contains many items whose trade is presumably controlled for commercial or social reasons as well as for national security considerations (as would apply to dual-use items). For example, the Chinese list includes items relating to animal husbandry and fisheries as well as software and computers. China has not published a control list covering weapons. Instead, arms can only be exported by 11 state-owned companies (which have their own internal control procedures).[28] As it is not possible to easily differentiate between weapons, military equipment, dual-use items and items controlled for other purposes, the discussion in the remainder of this section is based upon the EU, Norwegian and US military and dual-use control lists. It is though highly likely that China conceptualizes dual use in a similar fashion as it pursues similar policy goals and faces similar dilemmas.

Examination of the dual-use control lists provides some insight into how dual use is (implicitly) conceptualized in practice. Included in lists of dual-use equipment are: finished pieces of equipment; components of weapons and other military equipment; items used in testing, maintenance and production; specialized materials (such as certain alloys); software; and "technology" (e.g., technical data). Dual use covers the lifecycle of a weapon or piece of military equipment—its development, production and use. For example, items included in the EU, US and Norwegian control lists include components of a wide range of equipment including nuclear reactors, biological agents, robots, semiconductors, telecommunication systems, surveillance equipment, global positioning satellites, missiles and chemical and biological agents. We can assume from the items included in the lists that, in practice, "military use" is implicitly defined as *a role in actions specific to the military*. So, for example, food is not included as a dual-use item as eating is not a specifically military activity. Actions specific to military forces would clearly include combat and also related activities such as surveillance and reconnaissance. It appears that "military" is widely defined and includes use by members of security forces and intelligence agencies as well as the armed forces.

It is apparent that there are two means by which an item could be classified as dual use. Firstly, it may have been designed with civil and military applications from the outset. For example, an aircraft engine may have been developed for use in civil airliners and in military aircraft with similar specifications (for example, a maritime patrol plane). In this sense, being dual use is an

inherent aspect of the technology. Secondly, technology may be used in a different context to how it was originally developed. In some cases, purely military technology may diffuse out into civilian applications until the latter may be the most preponderant form of use. For example, radar was originally developed to detect enemy aircraft and naval vessels. Contemporary uses are much broader, and radar is an essential piece of safety equipment in civilian ships and aircraft. Types of radar are included in the Norwegian, United States and EU lists of dual-use equipment. A second change in context concerns equipment that was originally designed for civilian use but which is later found to have significant military applications. For example, in 2019 the EU Commission started a successful process to expand its definition of dual use to include "cyber-surveillance technologies" that had already been developed by civilian companies.[29]

Both the terms "dual use" and "artificial intelligence" as elaborated in this section are broad categories that have blurred borders whose composition is decided by the context in which items are used as well as by intrinsic qualities of the technology. For example, a microchip may be used for many different tasks, one of which could be to run AI software. A pattern recognition algorithm could be a key component of a weapon if it is used to identify and select targets. But, at least in principle, if such an algorithm were to be adapted for use in medicine to be used to identify cancer cells then it might be best classified as a dual-use product.

The difficulties in classifying and identifying AI dual-use technology pose profound challenges for regulators in China, the EU and the United States. In the past, controlled goods were usually physical objects whose trade could be monitored by customs officers stationed at ports. Dual-use AI technology poses several problems for trade controls as key aspects of the technology are based upon software. Specifically, this entails the following complications for those trying to control the trade in these items:

- The software component is intangible and thus very easy to transfer across borders and so avoid monitoring by customs officials and others involved in enforcing trade controls.

- The AI software will be written on perhaps tens or hundreds of thousands of lines of code. As such, it will be very difficult for an external party to verify the capabilities of a particular system.

- Software can be rapidly updated, so an initial export may not be of a controlled item, but a subsequent update to part of the software could cross the threshold. This is a problem for ensuring compliance with the regulations. It is a much greater concern for attempts to prevent certain actors obtaining AI technology.

- In common with other programs, AI software is now being offered as a service rather than as a standalone product which is definitively exported. AI services may be used by

clients operating in many different countries with consequent difficulties in controlling who uses the AI system that has been developed.

- General purpose AI programs are widely available, and so trade controls on general purpose software are likely to be ineffective and could harm the US, EU or Chinese technology sectors if they inhibit exports for commercial applications. It may be more feasible to restrict exports of AI software specifically designed for military applications (if this can be adequately defined and identified).

This occurs when they regulate the production and trade of some dual-use items (and, in doing so, produce lengthy lists of dual-use items), in particular materials (such as uranium) that could be used in weapons or weapon systems, including nuclear, chemical and biological weapons.

2. Developing and Regulating Dual-Use AI Technology: China, the US and the EU

While several countries are currently pursuing research in dual-use AI technology, we focus on China, the US and the EU because the former two have emerged as the main actors in developing this technology; the latter is attempting to dominate global efforts to regulate dual-use AI. These developments are happening against the background of an ongoing competition for technology dominance, which will have significant effects on the future balance of military power.

In October 2021, the US National Counterintelligence and Security Center (NCSC) warned that "U.S. leadership in emerging technology sectors faces growing challenges from strategic competitors who recognize the economic and military benefits of these technologies and have enacted comprehensive national strategies to achieve leadership in these areas. … [W]ith a more level technology playing field anticipated in the future, new technological developments will increasingly emerge from multiple countries and with less warning. While the democratization of such technologies can be beneficial, it can also be economically, militarily, and socially destabilizing."[30] The NCSC identifies China as the "primary strategic competitor to the United States because it has a well-resourced and comprehensive strategy to acquire and use technology to advance its national goals."[31]

Indeed, in its attempt to leapfrog the US and Europe and achieve dominance in dual-use technology, China is said to be building a techno-authoritarian state, and, thanks to a "whole-of-government" approach, it is now leading the field in selected industries.[32] For instance, China is amassing large amounts of data from both inside and outside of its borders, not the least through its Belt and Road Initiative (BRI) and its digital component, the Digital Silk Road (DSR). The latter, announced in 2015 as a way to enhance global digital connectivity, has become a central part of China's overall BRI strategy. It provides investments in high-tech developments, including recipients' AI capabilities, telecommunications networks, surveillance technology, cloud computing, e-commerce and Smart City programs.[33] China's ability to collect, store and utilize data through this and other initiatives may turn into a strategic advantage in leveraging information for AI applications in defense.[34]

As we highlight below, China plans to leverage AI as part of its plans to build highly technological weapons that would seriously challenge US armed forces (especially in the Indo-Pacific). Generally, the Chinese government seems to have so far focused on developing airborne robotic systems (including stealth drones similar to the US' X-47B); furthermore, efforts have been directed mostly at improving the effectiveness of existing systems by equipping them with further autonomy, although China is also looking into developing new and more innovative systems.[35] Commercial advancements in dual-use technology have also been beneficial to the defense sector. For instance, the company SubBlue, which produces undersea robotic systems for both commercial and defense applications, has recently established a partnership with the Tianjin Binhai AI Military-Civil Fusion Center, while the company ADASpace is producing AI-enabled satellites employing data processing capabilities.[36] According to some, such advancements will

allow China to conduct AI warfare in such a way as to ensure battlefield "brain supremacy," for instance through "focusing on intelligence supremacy, ubiquitous AppCloud, multi-domain integration, brain-machine fusion, intelligent autonomy, and unmanned combat."[37]

Against this background, in this section we unpack how China, the US and the EU are developing and regulating dual-use AI technology. As mentioned, China has been investing heavily in AI and automation. While these technologies are primarily civilian in their use, the Chinese Communist Party (CCP) has also been eager to exploit their relevance to defense and military applications. This has led the US and the EU to also step up their own efforts in the research and development of dual-use technology.

2.1. China

According to some analysts, China may have an advantage in developing dual-use AI technologies due to a number of domestic enabling factors, such as the "military-civil fusion" strategy, several national laws and Party guidelines, as well as local initiatives implemented in a number of provinces and cities.[38] The "military-civil fusion" (*junmin ronghe*) strategy has emerged as a key driver of the technological competition between the US and China.[39] The strategy is part of the CCP's plan to develop the People's Liberation Army (PLA) into a "world-class military" by mid-century.[40] Under this policy, private companies that develop new technologies are incentivized to share them with the Chinese government in order to incorporate them into military programs, and vice versa.[41] CCP committees have been implanted into over 35 tech giants to ensure that the companies' objectives align with the Party's, and in 2017 the government established the Central Commission for Integrated Military and Civilian Development, tasked with overseeing and coordinating military-civil fusion efforts.[42] It is however important to acknowledge that such a fusion remains aspirational and is hardly a reflection of the reality on the ground in China, an issue to which we return in Section 3.[43]

So far, the Central Military Commission has not released any official policy clarifying priorities in this field. However, several official documents and directives from the CCP give us a good sense of the push for innovation that is motivating China's politics today. For instance, China's 14th Five-Year Plan emphasizes technological innovation as a national strategic imperative and encourages the development of cutting-edge technologies, including AI, quantum computing, semiconductors, genetic research and biotechnology, space and deep sea and polar exploration.[44] The 2017 New Generation Artificial Intelligence Development Plan or AIDP (*Xin yidai rengong zhineng fazhan guihua*) calls for China to "strengthen the use of new-generation AI technology for command decision-making, military deductions, and national defense equipment."[45] This document lays out a three-step strategy to lead China's AI development; by 2030, China should become the global center for AI technologies, with a total expected value of RMB 1 trillion for core AI industries and RMB 10 trillion for AI-related industries.[46]



Rendering of Guizhou Soar Dragon high-altitude, long range UAV. Photo: Times Asi / Flickr

Furthermore, over the last few years the government has updated or adopted a number of laws that compel companies to participate in military-civil fusion efforts and aim to accompany and boost technological development. These include the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Internet Information Service Management Rules, the National Intelligence Law and, most recently, the Internet Information Service Algorithmic Recommendations Management Provisions. An examination of each of these is beyond the scope of this report, but the 2017 Cybersecurity Law for instance aims to establish clear guidelines for network security, protecting the rights of citizens and organizations and promoting technological development.[47] The law requires that any data collected in China must be stored in China, and companies must undergo security checks conducted by the government. Critics of this law point to its ambiguous nature and formulation and argue that such provisions increase the risk of security breaches and loss of information.[48]

These policies also go hand in hand with the China Standards 2035 plan, a strategy that outlines China's plan to write domestic and global standards for the manufacturing, exchange and consumption of the next generation of technology, including 5G networks, the Internet of Things (IoT) and AI.[49] These refer to industry standards, namely "a set of criteria within an industry relating to the standard functioning and carrying out of operations in their respective fields of production. In other words, it is the generally accepted requirements followed by the members of an industry."[50] This strategy is considered to be a follow up and an endorsement of the previously announced

Made in China 2025 Plan, an industrial policy that was meant to support the development of emerging technologies in the country, with the aim to transform China into a leading technology innovator and producer.[51] On the one hand, therefore, the new plan signals the importance leaders attach to seeing China taking the driving seat in the next industrial revolution. On the other hand, however, it is important to distinguish between posturing and real risks. For instance, the notion that the Chinese government is able to convince the world to adopt voluntary standards that are meant to bring advantages to Chinese companies is, for the time being, a stretch.[52]

Alongside efforts to boost China as a leader in developing and producing new technologies, the government is striving to regulate the field. In late 2020, Beijing approved the Export Control Law, which created a framework for restricting exports of military and dual-use products and technology for national security and public policy reasons. In the law, dual-use items are defined as "goods, technologies, and services that have both civil and military purposes or contribute to enhancing military potential, especially those that may be applied to design, develop, produce, or use weapons of mass destruction and their means of delivery."[53] Specific technological areas included are: unmanned aerial vehicles (UAVs), information processing technologies—for instance personal interactive data algorithms, intelligent scoring—and cyber-related technologies.

The law defines China's export control authorities as a joint mechanism under both the State Council and the Central Military Commission performing export control functions. According to a study by the US Congressional Research Service, "the final language includes several new provisions that appear aimed at creating a Chinese policy counterweight to the U.S. government's use of export control authorities to restrict the transfer of U.S. dual-use technology to China, including provisions for retaliatory action and extraterritorial jurisdiction."[54]

The law essentially authorizes the Chinese government to "exercise export controls in retaliation against other countries' actions, to impose temporary (up to two years) export controls on items not on a control list, and to broadly justify actions with several open-ended clauses" and it "includes provisions for China's participation in international discussions and regimes and global rulemaking on export controls according to the principles of equality and reciprocity, a sign that China could become more active in trying to set rules and norms that advantage China."[55] Even though it does not target any specific country, the law outlines clearly that the Chinese government will adopt measures to respond to export restrictions set by other countries toward China, thus appearing to set the legal basis for Beijing to respond to export control measures adopted by the US, such as when it targeted companies such as Huawei and the Semiconductor Manufacturing International Corporation.[56]

In April 2021, China's Ministry of Commerce (MOFCOM) issued the Guiding Opinions on Establishing the Internal Compliance Mechanism for Export Control by Exporters of Dual-use Items, which includes new Dual-Use Item Export Control Internal Compliance Guidelines (ECC

Guidelines).[57] The Opinions set nine basic elements to be included in an internal compliance program for export control; these elements are similar to those provided in the compliance guidelines for the Export Management and Compliance Program (EMCP Guidelines), published by the US Commerce Department Bureau of Industry and Security (BIS).[58] Only over time and by looking at the application of specific cases will it be possible to draw conclusions on the effects and impact of the Compliance Guidelines.

2.2. The US

The US intelligence and security community views AI "as the quintessential 'dual-use' technology," though, until recently, the US approach to AI lacked a governmental strategy, instead emphasizing private sector innovation without too much involvement from the state.[59] The 2019 American Artificial Intelligence Initiative and subsequent government documents focus heavily on protecting US leadership in AI technology, whilst simultaneously restricting flows of data and talent across borders.[60] The 2021 defense budget includes a big increase in spending for civilian AI research and development (R&D) (nearly USD 2 billion), with a plan to double it by 2022. Regarding defense/military AI, the Defense Advanced Research Projects Agency (DARPA) was set to invest US 459 million in AI R&D in 2021, and the DoD's Joint AI Center also increased its budget to USD 290 million.[61]



A US Air Force RQ-1 Predator Unmanned Aerial Vehicle. Photo: U.S. National Archives

In January 2021, the White House launched its National AI Initiative Office, which is tasked with "overseeing and implementing the United States national AI strategy and will serve as the central hub for Federal coordination and collaboration in AI research and policymaking across the government, as well as with private sector, academia, and other stakeholders."[62]

Additionally, the Department of Defense (DoD) has been conducting studies of potential military applications of AI since at least 2014, though it was not until 2018 that it launched its Joint AI Center (JAIC), the focal point of the Department's approach to AI.[63] In 2019, the DoD declassified a summary of its 2018 strategy on AI, which pointed to AI as playing a fundamental role in deterrence and maintaining the US' competitive military advantage over adversarial states.[64] The stated goals of the strategy are to: create opportunities to develop cutting-edge applications of AI; provide comprehensive training and cultivate talent in the workforce; complement the existing workforce with new skills and roles in the fields of machine learning, data engineering and data science (among others); and to build a culture that promotes experimentation.[65] The Joint AI Center will support the implementation of the DoD's strategy, helping in particular with strengthening existing military applications and enhancing future R&D efforts on AI; establishing a common foundation for scaling the impact of AI across the Department; and attracting and cultivating AI experts to guide education and training programs.[66] In a recent presentation at the US Naval Academy (Annapolis, Maryland), General Michael S. Groen, Director of JAIC, explained that AI is essential to the "establishment of a unified, integrated data flow throughout the chain of command." In this way, "AI is transformative because it accelerates decision cycles, operational responses, and force management," "integrates multiple feeds of intelligence," enhances "platform agility" by moving "the brain from one platform to another," "aids in threat recognition based on mobile cooperative and autonomous sensors," and enables "deconfliction of one's own forces, getting them out of the battlespace before the attack begins."[67]

Tasked with providing the US President and Congress with recommendations on the impact of artificial intelligence and other related technologies on US national security and defense, the bipartisan National Security Commission on Artificial Intelligence (NSCAI) published its final report in early 2021.[68] From early on, China and Russia have been presented as the biggest threats to America's technological predominance. What emerges from the report are recommendations for the US to invest substantially in the field of AI to protect national security, promote prosperity and safeguard democracy and its future. In short, the document proposes "an integrated national strategy to reorganize the government, reorient the nation, and rally our closest allies and partners to defend and compete in the coming era of AI-accelerated competition and conflict."[69]

In particular, the first part of the report addresses the issue of "defending America in the AI era" and presents AI-enabled capabilities as central to an era of conflict and strategic competition—one in which the US "must be prepared to defend against" threats such as deepfakes and lethal drones used by rogue states, terrorists and criminals.[70] The second part of the report addresses

technological competition with China and proposes a number of measures to tackle this, including winning the global talent competition, accelerating AI innovation domestically, protecting the US' technology advantages and building a favorable international technology order.

Lastly, in early 2022 NATO launched a new research program, called Defence Innovation Accelerator for the North Atlantic (DIANA), with the aim of joining efforts from industry, start-up companies and academia in order to research new dual-use technologies. The program will focus on technologies such as AI, big data processing, quantum-enabled technologies, autonomy, biotechnology, novel materials and space.[71] A major goal guiding this initiative is also the attempt to maintain technological dominance over countries such as China and Russia.

In 2018, the US government began the regulatory process of bringing in new trade controls to prevent actors such as China and Russia from obtaining advanced AI technology developed in the US. Progress has been slow, and as of November 2021 only one AI software application has been added to the US export control regime (see below). Control of the trade in AI applications involves some inherent difficulties related to the intangibility of software. While the US government can implement new laws and regulations, it will be very difficult to verify the nature of what has been exported.

In general, the US can be assumed to impose trade controls for two reasons. The first is geopolitical and motivated by a desire to prevent rival states or actors from obtaining advanced technology developed in the United States or in Europe. Secondly, the US government may be seeking to use trade controls to promote the commercial advantage of US companies that are developing AI. Usually, an intention to impose controls needs to be balanced against any likely negative effects on industry. Compliance with regulations invariably imposes greater costs. More importantly, export controls will inevitably limit commercial exports of high technology items from the US or even Europe, as is the case for example with the world's most advanced chip-making machine that is produced in the Netherlands.[72] Trade controls could also limit China (for instance) from engaging with potential commercial partners if the sharing of proprietary industrial information would raise risks for US security interests.

The US has started a process of establishing more controls on the trade in AI products. In 2018 the US Department of Commerce published an Advanced Notice on Proposed Rulemaking (ANPRM) which sought feedback from US parties on companies involved in trade in emerging technologies which may be added to US lists covering the export, re-export, or in-country transfer of controlled goods.[73] Within the AI field, the following technologies were highlighted in the ANPRM:

- Neural networks and deep learning (e.g., brain modelling, time series prediction, classification);

- Evolution and genetic computation (e.g., genetic algorithms, genetic programming);
- Reinforcement learning;
- Computer vision (e.g., object recognition, image understanding);
- Expert systems (e.g., decision support systems, teaching systems);
- Speech and audio processing (e.g., speech recognition and production);
- Natural language processing (e.g., machine translation);
- Planning (e.g., scheduling, game playing);
- Audio and video manipulation technologies (e.g., voice cloning, deepfakes);
- AI cloud technologies;
- AI chipsets.

In addition to AI, 14 other emerging technologies were included in the ANPRM, and some are relevant to weapons using AI, such as position, navigation and timing technology; microprocessor technology; advanced computing technology; data analytics technology; quantum information and sensing technology; brain-computer interfaces; and advanced surveillance technologies.

The ANPRM was followed up in January 2020 with an announcement of the addition to the US Export Control classifications of Software Specially Designed to Automate the Analysis of Geospatial Imagery, which employs a trained Deep Convolutional Neural Network.[74] Further, in August 2020 the US Bureau of Industry and Security, published a further ANPRM on possible controls on "foundational technologies" relevant to national security.[75] This ANPRM did not specify a list of technologies, though its focus—which is upon advanced technology that could be used by China or Russia—would naturally include AI applications that could be used in military technology.

While restrictions on the arms trade have a long history, the modern system of US trade controls was introduced during the early phases of the Cold War in order to prevent the Soviet Union and its allies from obtaining advanced US-made strategic technology.

The more powerful AI applications require similarly more powerful computer hardware. One approach, which is mentioned in the above discussion on the ANPRM, is to control the trade in

specific AI chips. Doing so would circumvent many of the problems associated with the intangibility of software and may be effective if certain software needs to be run on a dedicated chip. Another option is to control exports of general hardware used for high-performance computing (something the US has done for decades). However, such restrictions are unlikely to prevent actors from acquiring powerful hardware from other sources.

In practice, trade controls implemented by the US on AI applications may have to be implemented via compliance by companies and not rely upon additional checks by customs or other government officials. This means that companies need to ensure that their employees know what software might be covered by the regulations and what restrictions apply, especially with regards to aspects of software development such as uploading software to cloud computing servers or transporting personal laptops across borders.

2.3. The EU

Through its funding mechanisms for research and development, several actors in the EU, including defense companies, have long been able to participate in continent-wide consortia aimed to develop security solutions employing dual-use technology.[76] According to Martins and Ahmad, as reflected in its research programs the EU views "improved security, advanced technology and industrial development as fully integrated," thus understanding dual-use technology as a way to advance innovation in the continent and to promote the bloc's strategic autonomy in security and defense.[77]

Regarding AI more specifically, the EU has highlighted it as a major strategic priority for the near future.[78] So far, its strategy regarding the development of AI technology has been primarily oriented towards setting ethical standards, supporting member states as well as the private sector to comply with such standards and mitigating potential ethical risks—an approach which the EU itself calls "human-centric."[79] The EU has the potential to leverage its robust regulatory and market power and use it to gain a competitive advantage for what it calls "trustworthy AI," a vision that centers on transparency, diversity and fairness and that could increase the bloc's digital sovereignty, allowing users more choice and more control while ensuring accountability and oversight.[80]

In April 2018, 24 European countries and Norway signed a Declaration of Cooperation on Artificial Intelligence to formalize their intention to respond collectively to the challenges and opportunities brought about by AI.[81] Shortly afterwards, the European Commission published its strategy for AI, which was followed by the appointment of a group of 52 experts from academia, civil society and industry (the High-Level Expert Group on AI, or HLEG), tasked with supporting the EU with its strategy.[82] In 2019, the HLEG published the Ethics Guidelines for Trustworthy Artificial Intelligence, where they define "trustworthy AI" as being lawful, ethical and robust.[83]

Building on these guidelines, the HLEG published a document titled "Policy and investment recommendations for trustworthy Artificial Intelligence," which provides recommendations for the sustainable development of AI technology.[84]

In 2020 the European Commission also published a white paper on AI, in which it proposes a framework for the development and use of AI within the bloc according to which the Commission is "committed to enabling scientific breakthrough, to preserving the EU's technological leadership and to ensuring that new technologies are at the service of all Europeans—improving their lives while respecting their rights."[85] Military applications of AI are not mentioned in the white paper (nor are other dual-use technologies or autonomous weapons). Emphasis is instead placed on international dialogue and the EU's potential leading role in developing an international governance framework.[86] In a 2019 blueprint, the European Defence Agency (EDA) outlined its strategy to promote and coordinate AI innovation across member states, including plans to identify and analyze applications within the scope of its own research work that are relevant for defense and that can be affected by AI.[87] Finally, in October 2020, the EU Parliament adopted a text titled "Framework of ethical aspects of artificial intelligence, robotics and related technologies," which includes a section on "Security and Defense." For our purposes, these lines from the text are well worth quoting:

> *93. [The EU Parliament] Considers that current and future security and defence-related activities within the Union framework will draw on AI, on robotics and autonomy, and on related technologies and that reliable, robust and trustworthy AI could contribute to a modern and effective military […]; stresses that the development of reliable AI in the field of defence is essential for ensuring European strategic autonomy in capability and operational areas; recalls that AI systems are also becoming key elements in countering emerging security threats, such as cyber and hybrid warfare both in the online and offline spheres; underlines at the same time all the risks and challenges of unregulated use of AI; notes that AI could be exposed to manipulation, to errors and inaccuracies;*
>
> *94. Stresses that AI technologies are, in essence, of dual use, and the development of AI in defence-related activities benefits from exchanges between military and civil technologies; highlights that AI in defence-related activities is a transverse disruptive technology, the development of which may provide opportunities for the competitiveness and the strategic autonomy of the Union;*
>
> *96. Underlines the importance of investing in the development of human capital for artificial intelligence, fostering the necessary skills and education in the field of security and defence AI technologies with particular focus on ethics of semi-autonomous and autonomous operational systems based on human accountability in an AI-enabled world; stresses in particular the importance of ensuring that ethicists in this field have appropriate skills and receive proper training.*

The EU earmarked some of its 2021–2027 budget for the creation of the European Defence Fund, which, among other tasks, will address "cutting-edge, interoperable defense technology and equipment in novel areas like artificial intelligence, encrypted software, drone technology or satellite communication" and allocate funds to "disruptive technologies and high-risk innovation."[88]

The EU has been taking a number of steps to increase the coordination and convergence of member states' export controls on dual-use items since the 1990s.[89] In the spring of 2021, the EU adopted new regulation on export controls of sensitive dual-use technologies, such as cyber-surveillance tools. The EU defines these items as "goods, software and technology that can be used for both civilian and military applications."[90] This will replace the bloc's export control system for dual-use items that has been in place since 2009. The regulation mainly aims to strengthen action on the non-proliferation of weapons of mass destruction, contribute to peace, security and stability, and protect human rights and international humanitarian law. The list of relevant items includes a wide range of categories, such as nuclear materials, electronics, computers, telecommunications, information security, lasers, marine and aerospace.[91]

Around the same time, the European Commission unveiled its Proposal for a Regulation on a European approach for Artificial Intelligence (the EU AI Act), which follows a risk-based approach and pursues the development of trustworthy AI.[92] The regulation would ban AI systems that create potential threats to the safety, livelihoods and rights of citizens, differentiating between "unacceptable risk," "high risk" and "low or minimal risk."

Implementation of these policies is left to member states, resulting in very diverse outcomes across the bloc. Partly, this is due to the fact that the member states view dual-use technologies as strategic and are thus reluctant to let EU institutions regulate them on their behalf.[93] This has led to some technologies—which are regarded as more critical or strategic—receiving more support and attention by the EU and the various member states, such as AI.

In its drive to acquire foreign technologies to push the development of its domestic industry, China has been targeting European countries that hold a competitive advantage over Chinese companies in the engineering and production of high-tech systems (i.e., in robotics and cyber security). Among the various tactics utilized by Beijing to access European technologies are investments into the continent's companies, cooperation agreements with a range of European organizations, cyber espionage and joint ventures with European firms that want to operate in the Chinese market.[94]

3. Strategic Implications for the Balance of Power

As has been shown so far, in the context of the current geostrategic rivalry, China, the US and the EU are each taking steps to develop and regulate dual-use AI technology. The US and its allies, including Japan, Taiwan and some European countries, have been tightening China's access to sensitive technologies, mostly through tougher export control procedures and licensing practices. Additionally, several countries have in the past few years banned or imposed restrictions on the participation of Chinese telecommunication firms, in particular Huawei, in national 5G networks.[95] These measures have been taken in light of the expectation that military applications of AI dual-use technology will fundamentally change military power and, in turn, affect the global balance of power.

The Russian invasion of Ukraine and subsequent EU and US sanctions have the potential to raise the stakes in this rivalry. As well as potential Chinese uses for dual-use AI technology, policy-makers in the EU and US also need to consider the risks that China may undermine sanctions by passing on hardware and software to Russia.

Developments within China are a source of concern especially among the policy and military community in the US (and to a lesser extent in Europe). In particular, there is a perception "that China's pursuit of AI technologies will threaten the unassailable first-mover advantage that the U.S. has in a range of dual-use—and military-specific—AI applications. Because of this perceived threat, Washington will likely consider even incremental progress by China through a military lens, and thus treat any progress as a national security threat."[96] As highlighted in the US Department of Defense's 2021 annual China Military Power Report to Congress, China has made efforts to "blur the line demarcating commercial versus military use" of AI, for instance, which presents an additional obstacle in the way of fruitful cooperation between the world's major powers in ensuring international peace.[97] The report also refers to China as the only competitor to the US that is capable of challenging the openness and stability of the international system through a combination of economic, diplomatic, military and technological means.[98] Furthermore, despite the trade and regulation mechanisms put in place by the US and the EU, as seen above, China has managed to acquire cutting-edge technology by investing in or purchasing foreign companies; in 2020, for instance, Chinese FDI in the US totaled USD 7.2 billion.[99]

However, while China's centralized and top-down approach to developing dual-use AI technology may give the country an advantage vis-à-vis the US and other Western powers, some point out that such a strategy is not without its flaws. Among the problems that have arisen is the management of funding directed to AI, which seems inefficient, often overinvesting in certain areas that are favored by the leadership but which may not have a correspondingly high market demand; it has also been argued that China is encountering a shortage of experienced professionals who can develop AI algorithms. The US' more measured pace in producing AI innovations in the military would thus prove more strategic in the longer term.[100]

Moreover, the trajectory in both the development and employment of AI-enabled and autonomous weapon systems in China is uncertain, at least based on publicly available sources. In particular, China's progress in developing AI military technology is "contingent upon the capacity to operationalize emerging weapon systems, which will require overcoming current technological and organizational challenges in testing, training, and concepts of operations."[101] Furthermore, it is unclear whether China's "rush" to develop and deploy this kind of weapon system corresponds to a similarly quick process for testing the safety and reliability of such systems, particularly under real operational conditions.[102] The Chinese military also lacks contemporary operational experience, which may lead to mistakes or unrealistic expectations about the use of technology in war.[103] Thus, as underlined earlier, there is a substantial gap between China's aspirations to realize an all-encompassing military-civil fusion and the actual capabilities the country might deploy in future battlefield situations.

Generally, it is easy to see how technology shapes the balance of power through both economic and military means, for instance by impacting a country's economic power and by influencing a country's ability to wage war; however, it is less clear how specific AI applications may translate into military power.[104]

Nonetheless, we can make some assumptions about the challenges that AI poses for strategic stability. Horowitz argues that AI applications have the potential to shape future conflicts in a number of macro ways, such as by increasing the speed with which countries can fight, and while there is uncertainty about specific AI military applications, such an acceleration of pace in conducting warfare can significantly disrupt organizational structures.[105] AI systems might also lead to changes in military strategy, for instance by substituting machines for humans in making certain decisions.[106] Furthermore, the perception of any progress in the domain of dual-use technology risks creating a "dual-use security dilemma." This may happen even to actors who aim to develop technology only for civil purposes and who may find themselves in an arms race due to other actors potentially viewing such technology as a threat to their national security.[107]

Dual-use technology thus creates yet another layer of uncertainty, since one cannot know whether any given item has been created with civilian or military purposes, thus increasing the risk of miscalculation and mistrust.[108] Additionally, Boulanin et al. discuss several developments in AI-related technologies that may destabilize nuclear deterrence relations, specifically in the areas of remote sensing; non-nuclear strategic strike; missile defense and anti-access/area denial (A2/AD); and autonomous nuclear weapon delivery.[109] Therefore, knowing or believing that one or several states are planning to incorporate and utilize AI technologies into their future military capabilities might prompt other countries to react with measures that undermine strategic relations, thus increasing the likelihood of future (nuclear) conflict.[110] Within the context of the current Sino-US rivalry, uncertainties around any progress either country might be making is likely

to have implications for the strategic balance of power. In particular, "China's pursuit of AI (especially dual-use capabilities) will fuel the perception (accurate or otherwise) in Washington that Beijing is intent on exploiting this strategically critical technology to fulfil its broader revisionist goals."[111]

Conclusion and Recommendations for Norway

Given the rapid pace of disrupting transitions and the ensuing competition that drives AI developments today, it is likely that, in the future, no single power will emerge entirely unchallenged or maintain an uncontested edge in technological dominance. On the one hand, military power might be transformed in unpredictable ways, leading to increased uncertainty globally. Competition with countries such as China and Russia might, as a result, become a long-term feature of international affairs. On the other hand, emerging technologies could contribute to maintaining security, for instance through enhanced intelligence, better access to information, and analysis and prediction of opponents, leading to mutual deterrence and reducing the risks of the security dilemma.

China is already spending more on AI research than the US, and there is a risk that the People's Republic of China will surpass Europe in its capabilities to develop dual-use AI technologies, mostly due to the lack of a strong and coordinated EU-wide strategy to promote and protect Europe's own technologies.[112] However, regardless of whether certain countries end up with similar levels of AI technology capabilities, it is how these countries use AI that will ultimately matter most for the future balance of power.[113]

These risks require countries around the world to make strategic choices today. Norway is an active participant in international institutions and fora where the opportunities and challenges of dual-use AI technology are discussed. Norway has had its own national strategy for AI since 2020, which covers the civilian and commercial sector, but not defense.[114] The document generally points to the opportunities of AI, particularly the potential for creating more effective business models and user-centric public sector services. The government commits to promoting and facilitating the development of trustworthy AI that is built on ethical principles and respect for human rights, democracy, integrity and privacy. The strategy commits the country to continued participation in "European and international forums to promote responsible and trustworthy use of AI."[115]

In light of this commitment, we put forward the following recommendations for Norway:

- It is imperative to conduct thorough research on global developments in dual-use AI technology. This will enable realistic assessments of the threat rhetoric so that reactive policies can be avoided.

- Norway should exercise special vigilance vis-à-vis the export of AI technologies to countries like Russia, to prevent it from using such technology to develop military AI systems.

- Norway should engage diplomatically (both bilaterally and multilaterally) on issues relating to AI technology, especially with the leaders in this field, namely the US and China.

- In order to assess the impact of export control provisions, Norway should closely monitor trade relations between China, the US and the EU, as well as other relevant actors such as Russia, India, Turkey and Israel.

- Norway should actively participate in the EU efforts to leverage regional competitive advantage, with the aim of promoting a more secure and peaceful world.

- Norway should pursue cooperation and partnerships with like-minded democratic countries on matters relating to dual-use and AI technologies.

- Norway should promote dialogue with and between China, the US and the EU on the ethical and safe development/use of dual-use AI technologies. This would include discussions around TEVV (Testing, Evaluation, Verification and Validation) for AI-enabled defense systems. ■

Notes

1. Robert H. Latiff (2017) *Future War: Preparing for the New Global Battlefield*. New York: Alfred A. Knopf.
2. Stuart J. Russell (2020) *Human Compatible: Artificial Intelligence and the Problem of Control*. New York: Penguin Books, 112.
3. Miles Brundage et al. (2018) 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation'. February.
4. National Institute of Standards and Technology (2019) 'U.S. LEADERSHIP IN AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools'; White House Office of Science and Technology Policy (2020) 'American Artificial Intelligence Initiative: Year One Annual Report'. The White House, 5 February.
5. European Commission (2021) '2030 Digital Compass: The European Way for the Digital Decade'.
6. EU Parliament Resolution (2020) 'Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies'. 20 October.
7. For example, Helen Livingstone (2022) 'Russia Accuses Nato of "Proxy War" in Ukraine as US Hosts Crucial Defence Summit', *The Guardian*, 26 April 2022, sec. World news.
8. Council Regulation (EU) (2022) 2022/328 of 25 February 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, 049 OJ L §.
9. Julien Nocetti (2020) 'The Outsider: Russia in the Race for Artificial Intelligence'. *Russie.Nei.Reports*, No. 34, IFRI, 8 December.
10. Ibid.
11. Committee on Foreign Relations, United States Senate (2020) 'The New Big Brother: China and Digital Authoritarianism'. 21 July.
12. High-Level Expert Group on Artificial Intelligence (2019) 'A Definition of AI: Main Capabilities and Scientific Disciplines': 6.
13. For example: Tyler Rogoway (2014) 'The Navy's Smart New Stealth Anti-Ship Missile Can Plan Its Own Attack'. *Jalopnik*, 12 April.
14. Other items can be used as tools to cause harm or damage even if that was not their intended purpose when they were designed or made and has not become a general use (for example, using an airliner to destroy a building). We describe this process as weaponization, or refer to the item has having been weaponized (e.g., that the airliner was weaponized when it was used as a tool of violence). We describe such items as being "improvised weapons." In general, use of improvised weapons to cause harm or damage is covered by the laws, regulations, norms and practices which concern the use of weapons. However, they are not usually considered to be controlled goods concerning their development, production or trade.

15. "Non-consensual" is added to contrast the harm intended by military action from actions caused by other activities, such as medicine, for instance, as when surgeons remove a diseased limb to save the life of the patient. In the latter case, harm is done but it is not intended, as it is for the good of the patient who consents to the operation.

16. Hannah Arendt (1970) *On Violence*. New York: Harcourt, Brace & World.

17. A legal definition of "weapon" has been proposed as follows: "an offensive capability that can be applied to a military object or an enemy combatant." See Justin McClelland (2003) 'The Review of Weapons in Accordance with Article 36 of Additional Protocol I'. *Revue Internationale de La Croix-Rouge/ International Review of the Red Cross* 85(850): 404; Boothby (2009) adds that the "means whereby this is achieved will involve a device, munition, implement, substance, object, or piece of equipment, and it is that device etc that is generally referred to as a weapon." See William Boothby (2009) *Weapons and the Law of Armed Conflict*. Oxford: Oxford University Press.

18. Janis Grzybowski; Nicholas Marsh & Matt Schroeder (2012) 'Piece by Piece Authorized Transfers of Parts and Accessories'. In Glenn MacDonald (ed.) *Small Arms Survey 2012: Moving Targets*. Cambridge: Cambridge University Press, 240–281.

19. We define the term military widely, and it includes use by members of security forces and intelligence agencies as a central part of their roles. Elsewhere, dual use is described as concerning items which can be used for beneficial and harmful purposes. Such definition may cover how the term is used in popular discussions. However, it is too vague to be useful.

20. European Union (2021) 'Regulation Of The European Parliament And Of The Council in Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast)'. 21 April.

21. See for example the lack of a general definition in the UN Register of Conventional Arms, the Convention on Certain Conventional Weapons or the Arms Trade Treaty (all of which specify certain weapons without defining the category as a whole).

22. Laurence Lustgarten (2020) *Law and the Arms Trade: Weapons, Blood and Rules*. Oxford, UK; New York, NY: Hart Publishing.

23. Marsh & Greene (2012): 163–82.

24. The Norwegian dual-use list can be found at: www.regjeringen.no/globalassets/departementene/ud/vedlegg/eksportkontroll/liste2_2019.pdf and the United States list of dual-use items and less sensitive military technology can be found at: www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

25. See: www.wassenaar.org.

26. The Norwegian dual-use control list can be found at: www.regjeringen.no/globalassets/departementene/ud/vedlegg/eksportkontroll/liste2_2019.pdf. The Norwegian list of military equipment can be found

at: www.regjeringen.no/globalassets/departementene/ud/vedlegg/eksportkontroll/liste1_forsvarsrelatert_2019.pdf; the EU's military list can be found at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020XG0313%2807%29; The United States Munitions List can be found at: https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121.

27. "'Zhongguo Jinzhi Chukou Xianzhi Chukou Jishu Mulu" Tiaozheng Neirong [China's Technology Export Restriction List - Updated Content]', 2020, extension://elhekieabhbkpmcefcoobjddigjcaadp/http://www.gov.cn/zhengce/zhengceku/2020-08/29/5538299/files/135c5cdd6baa46a986ac5e51a1a49ac3.pdf.

28. Yann Aubin & Arnaud Idiart (2016) *Export Control Law and Regulations Handbook: A Practical Guide to Military and Dual-Use Goods Trade Restrictions and Compliance*. 3rd edition. Alphen aan den Rijn: Kluwer Law International B.V.

29. European Parliament (2021) 'Review of dual-use export controls'. 20 July.

30. National Counterintelligence and Security Center (NCSC) (2021) 'Protecting Critical and Emerging U.S. Technologies from Foreign Threats'. October: 1.

31. Ibid.: 2.

32. Meia Nouwens & Helena Legarda (2018) 'China's Pursuit of Advanced Dual-Use Technologies'. *IISS*, 18 December.

33. Yong Huang (2019) 'Construction of Digital Silk Road Lights up BRI Cooperation'. *People's Daily*, 24 April.

34. Nouwens & Legarda (2018) 'China's Pursuit of Advanced Dual-Use Technologies'.

35. Kania, Elsa B. (2020) '"AI Weapons" in China's Military Innovation'. Global China, April. Brookings.

36. Kania & Laskai (2021) *Myths and Realities of China's Military-Civil Fusion Strategy*.

37. Bill Gertz (2018) 'China in Race to Overtake the US in AI Warfare'. *Asia Times*, 30 May.

38. Kania (2020) '"AI Weapons" in China's Military Innovation'; Allen (2019); Forrest E. Morgan et al. (2020).

39. Kania & Laskai (2021).

40. State Council, People's Republic of China (2017) 'Guowuyuan Guanyu Yinfa Xin Yidai Rengong Zhineng Fazhan Guihua de Tongzhi [State Council Notice on the Issuance of the New Generation AI Development Plan]'. 20 August; Xi, Jinping (2018) 'Xi Jinping: Kai Chuangxin Shidai Junmin Ronghe Shendu Fazhan Xin Jumian [Xi Jinping: Opening up a New Era of in-Depth Development of Military-Civilian Integration]', 2 March.

41. Ilaria Carrozza (2020) 'The Individual, the National, and the Global: New Connections in Times of China-US Confrontation'. *PRIO Blog*, 6 October.

42. Nouwens & Legarda (2018).

43. Kania & Laskai (2021).

44. Xinhua (2021) '(Lianghui Shouquan Fabu) "Shisiwu" Guihua He 2035 Yuanjing Mubiao Di Fazhan Huanjing, Zhidao Fangzhen He Zhuyao Mubiao [(The Two Sessions Are Authorized to Issue) The Development Environment, Guidelines and Main Goals of the "14th Five-Year Plan" and 2035 Long-Term Goals]'. 5 March.

45. State Council, People's Republic of China (2017) 'Guowuyuan Guanyu Yinfa Xin Yidai Rengong Zhineng Fazhan Guihua de Tongzhi [State Council Notice on the Issuance of the New Generation AI Development Plan]'. 20 August; see also CAICT (2020) 'Rengong Zhineng Zhili Baipishu [Artificial Intelligence Governance White Paper]'.

46. For more details, see China Innovation Funding (2020) 'State Council's Plan for the Development of New Generation Artificial Intelligence'; Please note how the line between AI core industry and AI-related industries is blurred, leaving room for interpretation. See Jinghan Zeng (2021) 'China's Artificial Intelligence Innovation: A Top-Down National Command Approach?' *Global Policy* 12(3): 399–409; Jeffrey Ding (2019) 'Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI'. Future of Humanity Institute, University of Oxford; It should be noted that while central policies and guidelines are certainly important, such plans are often driven by the contestation, competition and struggle for resources among domestic stakeholders rather than established through a top-down approach. See Zeng (2021) 'China's Artificial Intelligence Innovation'.

47. Government of China (2020) 'Zhonghua Renmin Gongheguo Chukou Guanzhi Fa [Export Control Law of the People's Republic of China]'. 18 October; New America (2017) 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)'; In 2021, the government also shared a draft plan for the development of China's cybersecurity industry, which remained open for public comments over a few days. The plan lists several specific cybersecurity technologies that the CCP is encouraging domestic companies to pursue. See Center for Security and Emerging Technology (2021) 'Open Solicitation of Opinions on the Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023) (Draft for Solicitation of Opinions)'. 13 September.

48. Lauren Maranto (2020) 'Who Benefits from China's Cybersecurity Laws?' CSIS, 25 June.

49. Xinhua (2018) 'Guojia Biaozhun Wei: Zheng Zhiding "Zhongguo Biaozhun 2035" [The National Standards Committee Is Formulating the "China Standards 2035"]'. 10 January.

50. DOE Directives, Guidance, and Delegations (n.d.) 'Industry Standard'. Accessed 10 August 2021.

51. China Briefing News (2020) 'The China Standards 2035 Plan: Is It a Follow-Up to Made in China 2025?'. 2 July. The Made in China 2025 policy was later buried by Chinese leaders after it raised concerns abroad that it would be used by the CCP to promote domestic tech champions by allowing them privi-

leges vis-à-vis foreign competitors.

52. Naomi Wilson (2020) 'China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype'. Council on Foreign Relations, 3 June.

53. Government of China (2020) 'Zhonghua Renmin Gongheguo Chukou Guanzhi Fa'.

54. Congressional Research Service (2020) 'China Issues New Export Control Law and Related Policies'. 26 October: 1.

55. Ibid.: 2.

56. China Briefing (2020) 'China's Export Control Law Explained'. *China Briefing News*, 9 November.

57. Nathan Bush & Ray Xu (2021) 'Convergence in China's New Export Compliance Guidelines'. *Lexology*, 19 May.

58. Pillsbury (2021) 'China's MOFCOM Issues Internal Export Control Program Guidelines'. *Pillsbury Law*, 12 May.

59. NCSC (2021) 'Protecting Critical and Emerging U.S. Technologies from Foreign Threats': 4; Erik Brattberg; Raluca Csernatoni & Venesa Rugova (2020) 'Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?' *Carnegie Endowment for International Peace Working Paper*, 9 July.

60. White House Office of Science and Technology Policy (2020) 'American Artificial Intelligence Initiative: Year One Annual Report'.

61. The White House (2020) 'President Trump's FY 2021 Budget Commits to Double Investments in Key Industries of the Future'. February.

62. The White House (2021) 'The White House Launches the National Artificial Intelligence Initiative Office'. January.

63. Lindsay Sheppard (2020) 'Accelerating the Defense Department's AI Adoption', Council on Foreign Relations, April.

64. United States Department of Defense (2018) 'Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity'.

65. Ibid.; see also Joint Artificial Intelligence Center (n.d.) 'Five Pillars of the DoD AI Strategy'.

66. US DOD (2018) 'Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity': 9–10. For a study of how the different approaches to emerging technologies and innovation within the Army, Navy and Airforce, see Zoe Stanley-Lockman (2021) 'From closed to open systems: How the US military services pursue innovation'. *Journal of Strategic Studies* 44(4): 480–514.

67. From a keynote address given at the 21st Annual McCain Conference, 21 April, US Naval Academy, James B. Stockdale Center for Ethical Leadership; notes taken by Greg Reichberg.

68. National Security Commission on Artificial Intelligence (2021) 'Final Report: National Security Commission on Artificial Intelligence'.

69. Ibid.: 8.

70. Ibid.: 9.

71. Science Business (2022) 'NATO to Launch €1B Fund for High Tech Start-Ups in Dual Use Technologies'. 12 April.

72. Don Clark (2021) 'The Tech Cold War's "Most Complicated Machine" That's Out of China's Reach'. *The New York Times*, 4 July, sec. Technology.

73. Federal Register (2018) 'Review of Controls for Certain Emerging Technologies'. 19 November.

74. Federal Register (2020) 'Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series'. 6 January. This control was introduced as a temporary measure but has been renewed each year since 2020.

75. Federal Register (2020) 'Identification and Review of Controls for Certain Foundational Technologies'. 27 August.

76. Bruno Oliveira Martins & Neven Ahmad (2020) 'The Security Politics of Innovation: Dual-Use Technology in the EU's Security Research Programme'. In Antonio Calcara; Raluca Csernatoni & Chantal Lavallée (eds) *Emerging Security Technologies and EU Governance*. Abingdon: Routledge, 58–73.

77. Ibid.: 65.

78. Brattberg; Csernatoni & Rugova (2020); similarly, NATO has signaled its interest in setting AI standards, but has encountered difficulties in coordinating the often diverging priorities and budgets of its member states. See Melissa Heikkila (2021) 'NATO Wants to Set AI Standards. If Only Its Members Agreed on the Basics.' *POLITICO*, 29 March.

79. Huw Roberts et al. (2021) 'China's Artificial Intelligence Strategy: Lessons from the European Union's "Ethics-First" Approach'. *SSRN Scholarly Paper*, 1 March. Rochester, NY: Social Science Research Network; Brattberg; Csernatoni & Rugova (2020).

80. Brattberg; Csernatoni & Rugova (2020).

81. European Commission (2018) 'EU Declaration on Cooperation on Artificial Intelligence'. 10 April; more countries joined since then; see Roberts et al. (2021) 'China's Artificial Intelligence Strategy'.

82. European Commission (2018) 'Artificial Intelligence for Europe'. 25 April.

83. European Commission (2019) 'Ethics Guidelines for Trustworthy AI'. 8 April.

84. European Commission (2019) 'Policy and Investment Recommendations for Trustworthy Artificial Intelligence'. 26 June; for other relevant documents, see also European Commission (2019) 'The First European AI Alliance Assembly'; European Commission (2019) 'Liability for Artificial Intelligence and Other Emerging Digital Technologies'.

85. European Commission (2020) 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust'. 19 February: 1.

86. Roberts et al. (2021) 'China's Artificial Intelligence Strategy'; Brattberg; Csernatoni & Rugova (2020).

87. European Defence Agency (2020) 'Artificial Intelligence: Joint Quest for Future Defence Applications'. 25 August; on cybersecurity, see also European Union Agency for Cybersecurity (2020) *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence*. LU: Publications Office.

88. Internal Market, Industry, Entrepreneurship and SMEs - European Commission (2019) 'EU Budget for 2021-2027: Commission Welcomes Provisional Agreement on the Future European Defence Fund'. 20 February.

89. Mark Bromley & Kolja Brockmann (2021) 'Implementing the 2021 Recast of the EU Dual-Use Regulation: Challenges and Opportunities'. EU Non-Proliferation and Disarmament Consortium, September.

90. Council of the EU (2021) 'Trade of Dual-Use Items: New EU Rules Adopted'. 10 May.

91. European Union (2021) 'Regulation Of The European Parliament And Of The Council in Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast)'.

92. European Commission (2021) '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'. 21 April.

93. Nouwens & Legarda (2018).

94. Ibid.

95. Congressional Research Service (2020) 'China Issues New Export Control Law and Related Policies': 1.

96. James Johnson (2021) 'The End of Military-Techno Pax Americana? Washington's Strategic Responses to Chinese AI-Enabled Military Technology'. *The Pacific Review* 34(3): 351–78.

97. United States Department of Defense (2020) 'Military and Security Developments Involving the People's Republic of China 2020'. *Annual report to Congress*: XI.

98. Ibid.; Lauren Kahn (2022) 'What the Defense Department's 2021 China Military Power Report Tells Us About Defense Innovation'. *Lawfare*, 15 February.

99. Ibid.

100. Johnson (2021) 'The End of Military-Techno Pax Americana?': 365.

101. Kania (2020) '"AI Weapons" in China's Military Innovation'.

102. China Innovation Funding (2020) 'State Council's Plan for the Development of New Generation Artificial Intelligence'.

103. Kania (2020) '"AI Weapons" in China's Military Innovation'.

104. William Hardy McNeill (1993) *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*. Chicago: University of Chicago Press.; Michael C. Horowitz (2018) 'Artificial Intelligence, International Competition, and the Balance of Power'. *Texas National Security Review* 1(3): 36–57.

105. Horowitz (2018) 'Artificial Intelligence, International Competition, and the Balance of Power'; see also, Michael C. Horowitz & Paul Scharre (2021) 'AI and International Stability: Risks and Confidence-Building Measures'. Center for New American Security, January.

106. Horowitz & Scharre (2021) 'AI and International Stability: Risks and Confidence-Building Measures'.

107. Amir Lupovici (2021) 'The Dual-Use Security Dilemma and the Social Construction of Insecurity'. *Contemporary Security Policy* 42(3): 257–85.

108. For more specific risks due to the uses and limitations of AI in warfare, see Horowitz & Scharre (2021) 'AI and International Stability: Risks and Confidence-Building Measures'; and Vincent Boulanin; Lora Saalman, Petr Topychkanoz, Fei Su & Moa Peldán Carlsson (2020) 'Artificial Intelligence, Strategic Stability and Nuclear Risk'. SIPRI.

109. Boulanin et al. (2020). The authors also highlight some positive effects of AI on strategic stability. See pages 102–103.

110. Ibid.

111. James Johnson (2019) 'Artificial Intelligence & Future Warfare: Implications for International Security'. *Defense & Security Analysis* 35(2): 147–69.

112. Nouwens & Legarda (2018).

113. Horowitz (2018) 'Artificial Intelligence, International Competition, and the Balance of Power'; Johnson (2019) 'Artificial Intelligence & Future Warfare'.

114. Norwegian Ministry of Local Government and Modernisation (2020) 'National Strategy for Artificial Intelligence'.

115. Ibid.: 8.

Bibliography

Aubin, Yann & Arnaud Idiart (2016) *Export Control Law and Regulations Handbook: A Practical Guide to Military and Dual-Use Goods Trade Restrictions and Compliance*. 3rd edition. Alphen aan den Rijn: Kluwer Law International B.V.

Allen, Gregory C. (2019) 'Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security'. Center for a New American Security, 6 February.

Arendt, Hannah (1970) *On Violence*. New York: Harcourt, Brace & World.

Boothby, William (2009) *Weapons and the Law of Armed Conflict*. Oxford: Oxford University Press. DOI: 10.1093/acprof:oso/9780199569946.001.0001.

Boulanin, Vincent; Lora Saalman, Petr Topychkanoz, Fei Su & Moa Peldán Carlsson (2020) 'Artificial Intelligence, Strategic Stability and Nuclear Risk'. SIPRI.

Brattberg, Erik; Raluca Csernatoni & Venesa Rugova (2020) 'Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?' *Carnegie Endowment for International Peace Working Paper*, 9 July. Accessed 15 April 2021.
Available at: carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236.

Bromley, Mark & Kolja Brockmann (2021) 'Implementing the 2021 Recast of the EU Dual-Use Regulation: Challenges and Opportunities'. EU Non-Proliferation and Disarmament Consortium, September.

Brundage, Miles; Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe et al. (2018) 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation'. February.

Bush, Nathan & Ray Xu (2021) 'Convergence in China's New Export Compliance Guidelines'. *Lexology*, 19 May.
Available at: www.lexology.com/library/detail.aspx?g=1171cc70-ae52-4215-922e-c8bd406e0689.

CAICT (2020) 'Rengong Zhineng Zhili Baipishu [Artificial Intelligence Governance White Paper]'.
Available at: www.caict.ac.cn/kxyj/qwfb/bps/202009/t20200928_347546.htm.

Carrozza, Ilaria (2020) 'The Individual, the National, and the Global: New Connections in Times of China-US Confrontation'. *PRIO Blog*, 6 October.
Available at: blogs.prio.org/2020/10/the-individual-the-national-and-the-global-new-connections-in-times-of-china-us-confrontation.

China Briefing (2020) 'China's Export Control Law Explained'. *China Briefing News*, 9 November.
Available at: www.china-briefing.com/news/chinas-export-control-law-explainer-china-briefing-news.

China Briefing News (2020) 'The China Standards 2035 Plan: Is It a Follow-Up to Made in China 2025 ?'. 2 July.
Available at: www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals.

China Innovation Funding (2020) 'State Council's Plan for the Development of New Generation Artificial Intelligence'.
Available at: chinainnovationfunding.eu/dt_testimonials/state-councils-plan-for-the-development-of-new-generation-artificial-intelligence.

China Securities Regulatory Commission (2018) 'Zhonghua Renmin Gongheguo Wangluo Anquan

Fa [Cybersecurity Law of the People's Republic of China]'. 18 May.
Available at: www.csrc.gov.cn/pub/newsite/flb/flfg/flxzsf/201805/t20180518_338285.html.

Clark, Don (2021) 'The Tech Cold War's "Most Complicated Machine" That's Out of China's Reach'. *The New York Times*, 4 July, sec. Technology.
Available at: www.nytimes.com/2021/07/04/technology/tech-cold-war-chips.html.

Committee on Foreign Relations, United States Senate (2020) 'The New Big Brother: China and Digital Authoritarianism'. 21 July.

Congressional Research Service (2020) 'China Issues New Export Control Law and Related Policies'. 26 October.
Available at: extension://bfdogplmndidlpjfhoijckpakkdjkkil/pdf/viewer.html?file=https%3A%2F%2Fcrsreports.congress.gov%2Fproduct%2Fpdf%2FIN%2FIN11524.

Council Regulation (EU) (2022) 2022/328 of 25 February 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, 049 OJ L §.
Available at: data.europa.eu/eli/reg/2022/328/oj/eng.

Council of the EU (2021) 'Trade of Dual-Use Items: New EU Rules Adopted'. 10 May.
Available at: www.consilium.europa.eu/en/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted.

Center for Security and Emerging Technology (2021) 'Open Solicitation of Opinions on the Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021–2023) (Draft for Solicitation of Opinions)'. 13 September.
Available at: cset.georgetown.edu/publication/open-solicitation-of-opinions-on-the-three-year-action-plan-for-the-high-quality-development-of-the-cyber-security-industry-2021-2023-draft-for-solicitation-of-opinions.

Ding, Jeffrey (2019) 'Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI'. Future of Humanity Institute, University of Oxford.

DOE Directives, Guidance, and Delegations (n.d.) 'Industry Standard'. Accessed 10 August 2021.
Available at: www.directives.doe.gov/terms_definitions/industry-standard.

European Commission (n.d.) 'Dual-Use Trade Controls'. Accessed 10 August 2021.
Available at: ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls.

European Commission (2021) '2030 Digital Compass: The European Way for the Digital Decade'. 9 March.
Available at: ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf.

European Commission (2021) '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'. 21 April.
Available at: digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.

European Defence Agency (2020) 'Artificial Intelligence: Joint Quest for Future Defence Applications'. 25 August.

Available at: eda.europa.eu/news-and-events/news/2020/08/25/artificial-intelligence-joint-quest-for-future-defence-applications.

European Commission (2020) 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust'. 19 February.
Available at: ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission (2019) 'Ethics Guidelines for Trustworthy AI'. 8 April.
Available at: digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

European Commission (2019) 'Liability for Artificial Intelligence and Other Emerging Digital Technologies'.
Available at: op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en/format-PDF.

European Commission (2019) 'Policy and Investment Recommendations for Trustworthy Artificial Intelligence'. 26 June.
Available at: digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence.

European Commission (2019) 'The First European AI Alliance Assembly'.
Available at: digital-strategy.ec.europa.eu/en/events/first-european-ai-alliance-assembly.

European Commission (2018) 'Artificial Intelligence for Europe'. 25 April.
Available at: ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF.

European Commission (2018) 'EU Declaration on Cooperation on Artificial Intelligence'. 10 April.
Available at: ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence.

European Parliament (2021) 'Review of dual-use export controls'. 20 July.
Available at: www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2016)589832.

European Union (2021) 'Regulation Of The European Parliament And Of The Council in Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast)'. 21 April.

European Union Agency for Cybersecurity (2020) *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence*. LU: Publications Office.
Available at: data.europa.eu/doi/10.2824/238222.

EU Parliament Resolution (2020) 'Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies'. 20 October.
Available at: www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html.

Federal Register (2020) 'Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series'. 6 January.
Available at: www.federalregister.gov/documents/2020/01/06/2019-27649/addition-of-software-specially-designed-to-automate-the-analysis-of-geospatial-imagery-to-the-export.

Federal Register (2020) 'Identification and Review of Controls for Certain Foundational Technologies'. 27 August.

Available at: www.federalregister.gov/documents/2020/08/27/2020-18910/identification-and-review-of-controls-for-certain-foundational-technologies.

Federal Register (2018) 'Review of Controls for Certain Emerging Technologies'. 19 November.
Available at: www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

Gertz, Bill (2018) 'China in Race to Overtake the US in AI Warfare'. *Asia Times*, 30 May.
Available at: asiatimes.com/2018/05/china-in-race-to-overtake-the-us-in-ai-warfare.

Government of China (2020) '"Zhongguo Jinzhi Chukou Xianzhi Chukou Jishu Mulu" Tiaozheng Neirong [China's Technology Export Restriction List - Updated Content]'.
Available at: extension://elhekieabhbkpmcefcoobjddigjcaadp/http://www.gov.cn/zhengce/zhengceku/2020-08/29/5538299/files/135c5cdd6baa46a986ac5e51a1a49ac3.pdf.

Government of China (2020) 'Zhonghua Renmin Gongheguo Chukou Guanzhi Fa [Export Control Law of the People's Republic of China]'. 18 October.
Available at: www.gov.cn/xinwen/2020-10/18/content_5552119.htm.

Grzybowski, Janis; Nicholas Marsh & Matt Schroeder (2012) 'Piece by Piece Authorized Transfers of Parts and Accessories'. In Glenn MacDonald (ed.) *Small Arms Survey 2012: Moving Targets*. Cambridge: Cambridge University Press, 240–281.

Heikkila, Melissa (2021) 'NATO Wants to Set AI Standards. If Only Its Members Agreed on the Basics.' *POLITICO*, 29 March.
Available at: www.politico.eu/article/nato-ai-artificial-intelligence-standards-priorities.

High-Level Expert Group on Artificial Intelligence (2019) 'A Definition of AI: Main Capabilities and Scientific Disciplines'.

Horowitz, Michael C. (2018) 'Artificial Intelligence, International Competition, and the Balance of Power'. *Texas National Security Review* 1(3): 36–57. DOI: 10.15781/T2639KP49.

Horowitz, Michael C & Paul Scharre (2021) 'AI and International Stability: Risks and Confidence-Building Measures'. Center for New American Security, January.

Huang, Yong (2019) 'Construction of Digital Silk Road Lights up BRI Cooperation'. *People's Daily*, 24 April.
Available at: en.people.cn/n3/2019/0424/c90000-9571418.html.

Internal Market, Industry, Entrepreneurship and SMEs - European Commission (2019) 'EU Budget for 2021-2027: Commission Welcomes Provisional Agreement on the Future European Defence Fund'. 20 February.
Available at: ec.europa.eu/growth/content/eu-budget-2021-2027-commission-welcomes-provisional-agreement-future-european-defence-fund_en.

Joint Artificial Intelligence Center (n.d.) 'Five Pillars of the DoD AI Strategy'. Accessed 13 May 2022.
Available at: www.ai.mil/about.html.

Johnson, James (2019) 'Artificial Intelligence & Future Warfare: Implications for International Security'. *Defense & Security Analysis* 35(2): 147–69. DOI: 10.1080/14751798.2019.1600800.

Johnson, James (2021) 'The End of Military-Techno Pax Americana? Washington's Strategic Responses to Chinese AI-Enabled Military Technology'. *The Pacific Review* 34(3): 351–78. DOI:10.1080/09512748.2019.1676299.

Kahn, Lauren (2022) 'What the Defense Department's 2021 China Military Power Report Tells Us About Defense Innovation'. *Lawfare*, 15 February. Available at: https://www.lawfareblog.com/what-defense-departments-2021-china-military-power-report-tells-us-about-defense-innovation.

Kania, Elsa B. (2020) '"AI Weapons" in China's Military Innovation'. *Global China*, April. Brookings.

Kania, Elsa B. & Lorand Laskai (2021) 'Myths and Realities of China's Military-Civil Fusion Strategy'. Center for a New American Security, January.

Latiff, Robert H. (2017) *Future War: Preparing for the New Global Battlefield*. New York: Alfred A. Knopf.

Livingstone, Helen (2022) 'Russia Accuses Nato of "Proxy War" in Ukraine as US Hosts Crucial Defence Summit'. *The Guardian*, 26 April, sec. World news.
Available at: www.theguardian.com/world/2022/apr/26/russia-accuses-nato-of-proxy-war-in-ukraine-as-us-hosts-crucial-defence-summit.

Lupovici, Amir (2021) 'The Dual-Use Security Dilemma and the Social Construction of Insecurity'. *Contemporary Security Policy* 42(3): 257–85. DOI: 10.1080/13523260.2020.1866845.

Lustgarten, Laurence (2020) *Law and the Arms Trade: Weapons, Blood and Rules*. Oxford, UK; New York, NY: Hart Publishing.

Maranto, Lauren (2020) 'Who Benefits from China's Cybersecurity Laws?' *CSIS*, 25 June.
Available at: www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

Marsh, Nicholas & Owen Greene (2011) 'Governance and Small Arms and Light Weapons'. In Nicholas Marsh (ed.) *Small Arms, Crime and Conflict Global Governance and the Threat of Armed Violence*. London: Routledge, 163–182.

Martins, Bruno Oliveira & Neven Ahmad (2020) 'The Security Politics of Innovation: Dual-Use Technology in the EU's Security Research Programme'. In Antonio Calcara; Raluca Csernatoni & Chantal Lavallée (eds) *Emerging Security Technologies and EU Governance*. Abingdon: Routledge, 58–73.

McClelland, Justin (2003) 'The Review of Weapons in Accordance with Article 36 of Additional Protocol I'. *Revue Internationale de La Croix-Rouge/International Review of the Red Cross* 85(850): 397–415. DOI: 10.1017/S1560775500115226.

McNeill, William Hardy (1993) *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*. Chicago: University of Chicago Press.

Morgan, Forrest E.; Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima & Derek Grossman (2020) *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica, CA: RAND Corporation.

National Institute of Standards and Technology (2019) 'U.S. LEADERSHIP IN AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools'.
Available at: www.nist.gov/system/files/documents/2019/08/10/

ai_standards_fedengagement_plan_9aug2019.pdf.

National Security Commission on Artificial Intelligence (2021) 'Final Report: National Security Commission on Artificial Intelligence'.

New America (2017) 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)'. Accessed 18 November 2020.
Available at: newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china.

Norwegian Ministry of Local Government and Modernisation (2020) 'National Strategy for Artificial Intelligence'.

Nocetti, Julien (2020) 'The Outsider: Russia in the Race for Artificial Intelligence'. *Russie.Nei.Reports*, No. 34, IFRI, 8 December.
Available at: www.ifri.org/en/publications/etudes-de-lifri/russieneireports/outsider-russia-race-artificial-intelligence.

Nouwens, Meia & Helena Legarda (2018) 'China's Pursuit of Advanced Dual-Use Technologies'. *IISS*, 18 December.
Available at: www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance.

National Counterintelligence and Security Center (NCSC) (2021) 'Protecting Critical and Emerging U.S. Technologies from Foreign Threats'. October.

Pillsbury (2021) 'China's MOFCOM Issues Internal Export Control Program Guidelines'. *Pillsbury Law*, 12 May.
Available at: www.pillsburylaw.com/en/news-and-insights/china-mofcom-issues-internal-export-control-program-guidelines.html.

Roberts, Huw; Josh Cowls, Emmie Hine, Jessica Morley, Mariarosaria Taddeo, Vincent Wang & Luciano Floridi (2021) 'China's Artificial Intelligence Strategy: Lessons from the European Union's "Ethics-First" Approach'. *SSRN Scholarly Paper*, 1 March. Rochester, NY: Social Science Research Network.
Available at: papers.ssrn.com/abstract=3811034.

Rogoway, Tyler (2014) 'The Navy's Smart New Stealth Anti-Ship Missile Can Plan Its Own Attack'. *Jalopnik*, 12 April.
Available at: jalopnik.com/the-navys-smart-new-stealth-anti-ship-missile-can-plan-1666079462.

Russell, Stuart J. (2020) *Human Compatible: Artificial Intelligence and the Problem of Control*. New York: Penguin Books.

Science Business (2022) 'NATO to Launch €1B Fund for High Tech Start-Ups in Dual Use Technologies'. 12 April.
Available at: sciencebusiness.net/news/nato-launch-eu1b-fund-high-tech-start-ups-dual-use-technologies.

Sheppard, Lindsay (2020) 'Accelerating the Defense Department's AI Adoption', Council on Foreign Relations, April.
Available at: www.cfr.org/report/accelerating-defense-departments-ai-adoption.

Stanley-Lockman, Zoe (2021) 'From closed to open systems: How the US military services pursue innovation'. *Journal of Strategic Studies* 44(4): 480–514.

State Council, People's Republic of China (2017) 'Guowuyuan Bangong Ting Guanyu Tuidong Guofang Keji Gongye Junmin Ronghe Shendu Fazhan de Yijian [General Office of the State Council on Promoting National Defense Technology Industry. Opinions on the in-Depth Development of Military-Civilian

Integration]'.
Available at: http://www.gov.cn/gongbao/content/2017/content_5248218.htm.

State Council, People's Republic of China (2017) 'Guowuyuan Guanyu Yinfa Xin Yidai Rengong Zhineng Fazhan Guihua de Tongzhi [State Council Notice on the Issuance of the New Generation AI Development Plan]'. 20 August.
Available at: www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

The White House (2021) 'The White House Launches the National Artificial Intelligence Initiative Office'. January.
Available at: trumpwhitehouse.archives.gov/briefings-statements/white-house-launches-national-artificial-intelligence-initiative-office.

The White House (2020) 'President Trump's FY 2021 Budget Commits to Double Investments in Key Industries of the Future'. February.
Available at: trumpwhitehouse.archives.gov/briefings-statements/president-trumps-fy-2021-budget-commits-double-investments-key-industries-future.

United States Department of Defense (2020) 'Military and Security Developments Involving the People's Republic of China 2020'. *Annual report to Congress*.
Available at: media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

United States Department of Defense (2018) 'Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity'.

White House Office of Science and Technology Policy (2020) 'American Artificial Intelligence Initiative: Year One Annual Report'. The White House, 5 February.

Wilson, Naomi (2020) 'China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype'. Council on Foreign Relations, 3 June.
Available at: www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype.

Xi, Jinping (2018) 'Xi Jinping: Kai Chuangxin Shidai Junmin Ronghe Shendu Fazhan Xin Jumian [Xi Jinping: Opening up a New Era of in-Depth Development of Military-Civilian Integration]', 2 March.
Available at: www.gov.cn/guowuyuan/2018-03/02/content_5270143.htm.

Xinhua (2021) '(Lianghui Shouquan Fabu) "Shisiwu" Guihua He 2035 Yuanjing Mubiao Di Fazhan Huanjing, Zhidao Fangzhen He Zhuyao Mubiao [(The Two Sessions Are Authorized to Issue) The Development Environment, Guidelines and Main Goals of the "14th Five-Year Plan" and 2035 Long-Term Goals]'. 5 March.
Available at: www.xinhuanet.com/politics/2021lh/2021-03/05/c_1127172897.htm?mc_cid=f6cc063bc4&mc_eid=2700f9a08f.

Xinhua (2018) 'Guojia Biaozhun Wei: Zheng Zhiding "Zhongguo Biaozhun 2035" [The National Standards Committee Is Formulating the "China Standards 2035"]'. 10 January.
Available at: www.xinhuanet.com/fortune/2018-01/10/c_129787658.htm.

Zeng, Jinghan (2021) 'China's Artificial Intelligence Innovation: A Top-Down National Command Approach?' *Global Policy* 12(3): 399–409. DOI: 10.1111/1758-5899.12914.

Dual-Use AI Technology in China, the US and the EU

Strategic Implications for the Balance of Power

This report focuses on dual-use artificial intelligence (AI) technology as a central element in the current great power competition. It examines advances in developing and regulating dual-use AI technology in China, the European Union and the United States, and it considers the strategic implications of these developments for the balance of power. It concludes that while in the future no single power will emerge entirely unchallenged in the technological realm, countries need to make strategic choices that take into account both the opportunities and the risks associated with emerging technologies and their military applications.

Ilaria Carrozza
Peace Research Institute Oslo (PRIO)

Nicholas Marsh
Peace Research Institute Oslo (PRIO)

Gregory M. Reichberg
Peace Research Institute Oslo (PRIO)

