European Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/feus20

Artificial intelligence and EU security: the false promise of digital sovereignty

Andrea Calderaro & Stella Blumfelde

To cite this article: Andrea Calderaro & Stella Blumfelde (2022) Artificial intelligence and EU security: the false promise of digital sovereignty, European Security, 31:3, 415-434, DOI: 10.1080/09662839.2022.2101885

To link to this article: https://doi.org/10.1080/09662839.2022.2101885

Published online: 09 Sep 2022.

EUROPEAN SECURITY
2022, VOL. 31, NO. 3, 415–434
https://doi.org/10.1080/09662839.2022.2101885

OPEN ACCESS

Artificial intelligence and EU security: the false promise of digital sovereignty

Andrea Calderaro [a] and Stella Blumfelde [b]

[a]Department of Politics and International Relations, Cardiff University, Cardiff, UK; [b]Department of Political and International Science, University of Genoa, Genoa, Italy

ABSTRACT
EU Digital Sovereignty has emerged as a priority for the EU Cyber Agenda to build free and safe, yet resilient cyberspace. In a traditional regulatory fashion, the EU has therefore sought to gain more control over third country-based digital intermediaries through legislative solutions regulating its internal market. Although potentially effective in shielding EU citizens from data exploitation by internet giants, this protectionist strategy tells us little about the EU's ability to develop Digital Sovereignty, beyond its capacity to react to the external tech industry. Given the growing hybridisation of warfare, building on the increasing integration of artificial intelligence (AI) in the security domain, leadership in advancing AI-related technology has a significant impact on countries' defence capacity. By framing AI as the intrinsic functioning of *algorithms*, *data mining* and *computational capacity*, we question what tools the EU could rely on to gain sovereignty in each of these dimensions of AI. By focusing on AI from an EU Foreign Policy perspective, we conclude that contrary to the growing narrative, given the absence of a leading AI industry and a coherent defence strategy, the EU has few tools to become a global leader in advancing standards of AI beyond its regulatory capacity.

ARTICLE HISTORY
Received 24 November 2021
Accepted 12 July 2022

KEYWORDS
Digital sovereignty; artificial intelligence; EU security; EU foreign policy

Introduction

The call for EU Digital Sovereignty identifying the need to build free and safe, yet resilient cyberspace is increasingly at the centre of the EU agenda. These issues are consistent with the broader EU ambition to achieve "strategic autonomy", first announced in 2013 in regards to the defence industry (European Council, 2013), and later adopted for broader defence and security purposes with the launch of the European Union Global Strategy (EUGS) in 2016 (European External Action Services 2016). Clustered around the need to strengthen the EU's capacity and ability to protect itself as an actor in global politics as well as its citizens (European Commission 2020a) both within and outside its borders (Bellanova and Glouftsios 2022, Martins *et al.* 2022), this priority has developed

CONTACT Andrea Calderaro CalderaroA@Cardiff.ac.uk
This article has been corrected with minor changes. These changes do not impact the academic content of the article.

over the years of challenging external circumstances. The Snowden case, first, increased public concern with state-sponsored mass surveillance strategies, and digital privacy became a priority of a nascent EU digital agenda (Hintz *et al*. 2019). The subsequent Cambridge Analytica scandal, further highlighted the dominant role of digital intermediaries over states and society (Kapczynski 2019), with the increasing trend of economic exploitation of data (Zuboff 2019), and their interfering capacity in states' democratic equilibrium (York 2021). The market influence of private actors in what is traditionally state affairs pushed the EU to demand stronger regulations over digital services. Then, with growing tension in the transatlantic relationship during the Trump presidency, the EU initiated a string of initiatives to gain independence from the US-led digital market and assert a claim to EU Digital Sovereignty.

The emerging claim to Digital Sovereignty has been coupled with vibrant discussions on the role of AI, including on data mining, algorithms accountability and leadership in the tech industry, which has become a prominent feature in European efforts to achieve strategic autonomy. The 2022 Strategic Compass sets out the EU's ambition to become a global leader in AI by reducing the dependency on external actors for emerging technologies, increasing the production of high-performance computer processors and the establishment of an independent data space. Moreover, the document highlights how AI in the EU is expected to be a key component of a new European security and defence strategy as it shall be a part of future weapon systems (European Commission 2021a, European External Action Service 2022).

However, the growing narrative on EU Digital Sovereignty and the intensification of initiatives aiming at building EU leadership on AI, tell us little about the EU's actual capacity to achieve this goal. AI is still a foggy concept, turning the debate in the field into a cacophony of perspectives from both scholars and policymakers. Without a convincing framework of what AI really means, it is still difficult to identify what global leadership in AI implies and how it could be achieved. The EU is not immune to the general confusion in the field, and it has addressed sovereignty over AI in an increasing number of statements and strategies ranging from protectionist practices, claims to gain technology and innovation superiority, and ambition to achieve "tech-deterrence". However, as we argue in this article, we have little evidence that the EU will be able to pursue Digital Sovereignty and global leadership in the AI domain given the lack of major digital tech industry and investments when compared to the intensity in efforts by the leading actors in the AI domain, notably the US and China (Archibugi and Mariella 2021).

This article addresses how the EU is positioning itself in the race to dominate technological developments, and focuses on the implications of such positioning. In particular, we explore how the EU's ambition to lead technological developments in the field of artificial intelligence (AI) map onto the nascent concept of Digital Sovereignty. We approach AI as the intrinsic functional combination of three key elements: *data*, *algorithms* and *hardware*, which in the specific case of AI is referred to as *computational power*, and we argue that any country's ambition to gain sovereignty over AI is bound to its capacity to be sovereign over each of these elements. By adopting this lens to the EU case, this approach enables us to highlight the limited tools that the EU has to pursue its coveted global leadership in AI, and questions what kind of Digital Sovereignty the EU could achieve given the limited available tools.

The findings of the paper point to discrepancies between the EU's normative and legislative approach to protecting its digital market, on the one hand, and the practical steps taken towards the development of an EU global leadership in AI, on the other. As such, it highlights internal tension and possibly contradictions in the EU's understanding of Digital Sovereignty. We first look at the strategies that the EU has implemented to advance Digital Sovereignty by protecting its internal digital market and EU citizens' data from third countries-based tech industry. By focusing on the global rush to implement AI in defence strategies, we then compare the EU approach to other global competitors in this domain. With this approach, we emphasise how the lack of an EU-leading tech industry is not the only weakness for overcoming the current technological gap where the EU is cornered. While other countries are boosting their advancement in the tech sector by building on their security framework, the EU suffers from the lack of a consistent defence strategy. We, therefore, conclude that the EU is trying to overcome this gap and lack of short-term solutions by implementing protectionist regulatory tools, an approach that enables the EU to influence a field without being able to contribute to shape it.

The EU approach to Digital Sovereignty

In the EU context, Digital Sovereignty is often addressed under the umbrella of a broader initiative on "strategic autonomy" (Timmers 2019). The concept of strategic autonomy was introduced in the EU's global strategy in 2016 in which sovereignty was mainly used in the context of military, security and defensive discourse (European External Action Services 2016). Digital Sovereignty, however, entails a much wider meaning (see introduction to this issue Bellanova *et al*. 2022). European sovereignty has been referred to as the need to put the EU's "destiny into its own hands" and to the ambition to develop "the capacity to play a role in shaping global affairs" (Juncker 2018), yet it remains unclear how Digital Sovereignty is defined and operationalised. The concept is often used interchangeably with "technological sovereignty", mostly relating to normative and prescriptive ideas of control, autonomy and independence (Couture and Toupin 2019, Pohle and Thiel 2020). In particular, the Strategic Compass refers to Technological Sovereignty instead than Digital Sovereignty, as a key tool for mitigating strategic dependencies and preserving intellectual property (European External Action Service 2022).

Despite the lack of a consistent and clear definition, the call for Digital Sovereignty builds on the full dependency of the EU on external digital intermediaries and tech companies. So far, the lack of major EU tech companies has prevented the EU and its member states from being proactive in the race to technological global leadership. As a consequence, the EU strategy to achieve Digital Sovereignty has been sought with the intention not only to generate imaginaries of an EU leadership in the field (Csernatoni 2022, Lambach and Monsees 2022), but also by implementing protectionist initiatives, by which we mean the series of regulations designed to protect its internal digital market. As a result, EU Digital Sovereignty has been mostly tied to the idea of the EU as a regulatory actor in the international digital environment (Bradford 2020, Micklitz *et al*. 2021, Farrand and Carrapico 2022), impacting on the monopoly of US digital service providers and Chinese tech companies in the European market only.

We can identify early initiatives aiming at empowering the EU competencies over non-EU tech companies even before the more recent growing call for EU Digital Sovereignty. In line with the approach, we propose to frame AI Sovereignty, as the sovereignty over its core intrinsic elements, i.e. *data*, *algorithms* and *hardware*. We observe how the EU has traditionally adopted a regulatory approach to protect its digital market to be influential in the domain of digital innovation despite the lack of leadership in this sector.

Data. Looking at what we identify as the *first* core element of AI, sovereignty over data, with the 2012 European Data Protection Regulation, launching the discussion on the "right to be forgotten" (European Parliament 2012), one of the most significant steps to develop EU digital standards on privacy was implemented. This regulation has impact not only within, but also beyond EU borders, and in particular it enables the EU to impose digital privacy standards on US-based internet service. A few years later, the Snowden case further boosted the EU efforts to gain sovereignty by protecting EU citizens' data. The exposure of EU citizens' data to the US' mass surveillance strategy leaked by Snowden, pushed the EU to develop a concrete EU model of data mining to reinforce a European digital privacy framework against the so far Laisse-fair approach of the US. With the General Data Protection Regulation (GDPR) in 2016, the EU equipped itself with an additional tool to impose its standards over the data mining capacity of the private sector (Bradford 2020). In this case too, by focusing on the protection of privacy of EU citizens, the GDPR has a significant impact on internet standards given that any company, regardless of where it is based and accessed by EU citizens, should comply with the law (Li *et al*. 2019). The GDPR is a key example of how the EU has been able to overcome a lack of global leadership in the digital sector by implementing protectionist regulations targeting its digital market but simultaneously influencing the global debate on how to develop a human rights-based approach to digital strategies.

Algorithms. The proliferation of online Hate Speech generated concerns over the power of algorithms in locking the public's knowledge building into filter bubbles (Flaxman *et al*. 2016). Its impact on global security became evident when in the early 2010s the Islamic State of Iraq and Syria (ISIS) exploited such filter bubbles to boost its ideological propaganda and recruitment strategy (European Parliament and Council of the European Union 2018, Marsden *et al*. 2020). A few years later, the ensuing Cambridge Analytica scandal linked to the economic models adopted by US-based tech giants like Google and Facebook, illustrated the uncontrolled pattern of online user data exploitation and surveillance for commercial, health and political purposes (Woolley and Howard 2018). The Cambridge Analytica case shed light on the detrimental consequences of the dominant role of US-based tech giants not only over the privacy of EU citizens but also on the EU electoral system. The centrality that Tech Giants have gained in channelling the political debate was tied to their power in boosting misinformation campaigns with the consequent direct impact on EU electoral processes. In addition to data mining, the Cambridge Analytica case shifted attention to the *second* pillar of AI consisting of algorithms accountability and the weak EU control of these processes. The concurrent tensions in the US-Europe partnership during the Trump presidency provided further incentives to seek alternative ways to the status quo situation on AI. Not only because of the reluctance of the Trump administration to negotiate solutions aiming at solving the growing EU concerns related to the dominance of US-based digital intermediaries. Moreover, by announcing the charging of different tariffs on European imports and actual rejection of elements of the multilateral trading system (Azmeh et al. 2020), Trump effectively pushed the EU to further prioritise its ambition to build EU Digital Sovereignty by gaining independence from the US-led digital market.

Hardware. A more explicit call for EU Digital Sovereignty was laid out in a 2017 report by the European Union Agency for Cybersecurity (ENISA) before the release of the Digital Single Market. It warned about the critically high dependency of the EU on third country technology and the detected cases of state-sponsored surveillance and espionage, and called for protecting the EU's privacy, security and data through law and development of core products and competencies (ENISA 2017). In addition to the dominant position of US-based digital intermediaries in the EU digital market, the lack of algorithm accountability and transparency of data mining policy, attention shifted also to the potential threats emerging from non-EU digital tech hardware and related computational power, here identified as the *third* element of AI. In particular, the European Parliament expressed concerns about the potential security threats of embedded backdoors in 5G equipment provided by two key Chinese companies, Huawei and ZTE, that could allow unauthorised access to sensitive data and telecommunications (Friis and Lysne 2021). The statement supported the concern over third-country equipment vendors and emphasised the need to "develop a strategy aimed at reducing Europe's dependency on foreign technology in the field of cybersecurity" (European Parliament 2019). In order to react to the rapidly evolving debate on the urgency to achieve EU Digital Sovereignty, the European Commissioner, Ursula von der Leyen, launched her presidency in 2019 by emphasising that technological sovereignty can be achieved by having digital capacities such as quantum computing, 5G and AI, which are based on European values (von der Leyen 2019). Shortly later, the European Council followed up by stressing the need to ensure technological sovereignty through a digital single market, global regulatory power and strategic digital capacity and infrastructure (European Council 2020). These points were elaborated further in the Coordinated Plan on the Development of AI in Europe approved in 2021 (European Commission 2021b).

However, in contrast to this emerging narrative of a forceful EU *en route* to solidifying its control over Digital Sovereignty across the three core dimensions, AI's technical nature points to a very different picture. In particular, given the European tech industry's lack of ability to compete with the dominant US and Chinese companies, the EU appears disarmed in achieving the claimed global leadership in the AI domain (Mazzucato and Perez 2015). For this reason, the current Digital Sovereignty strategy of the EU (European Commission 2020b) largely mirrors the objectives and tools to achieve their goals set out in the Digital Single Market Strategy of 2015 and more recently renewed by the EU Commissioner for the internal market, Thierry Breton. The three pillars of the Digital Sovereignty announced by Breton (2020) are Data, Microelectronics, and Connectivity, referring to the EU ambition to gain more control over data mining and cloud services, develop an EU industry microchip industry, and secure its connectivity infrastructure. These priorities have been reinforced by the European Council calling for more rules, advancing technological capacity and safeguarding of European values to reach greater security (European Council 2020). The only difference between the previous and new strategies is the technology identified, which besides mentioning big data and cloud computing now also include AI, quantum computing and other recent technological developments (European Commission 2020b).

Furthermore, the Digital Strategy redundantly reaffirms the objectives and strategic steps to be taken towards greater autonomy, as already outlined in the digital agenda (European Commission 2021c).

Overall, according to initiatives that the EU has taken to achieve Digital Sovereignty, the economic pillar of the digital strategy is the most significant at achieving Digital Sovereignty as it foresees investment as an important part of the dependency problem. The announced investments could certainly provide results, but only in the long term, leaving the EU with little capacity to quickly bridge the technological gap with the US and China, and gain independency from them. In the short and medium term, similarly to the initiatives taken in the near past and discussed above, the EU can mostly rely on proxy measures consisting of regulatory tools adopted to protect the Digital Single Market.

From Normative Power Europe to the Brussels Effect

Building on the growing debate on norms shaping the EU context, by proposing the concept of Normative Power of the European Union, Manners (2002) aimed to build-up on the existent knowledge and offer greater understanding of the European integration processes. Even though normative power has been acknowledged as having been exercised by different actors such as the US, the EU is seen as an exceptional case based on its historic background which builds on "exceptional" failures and crimes of the past such as colonialism, world wars and holocaust (Manners and Diez 2007). By defining Normative Power Europe (NPE), Manners (2002) introduced normative power as an exclusive EU "ability to shape or change what passes for normal in international relations". Ever since the concept has been broadly applied across multiple dimensions of the EU's emerging areas of influence, exposing the concept to revision, adaptation and critique (Onar and Nicolaïdis 2013). It is however noteworthy how "sticky" this term has been, including among EU policy makers.

More recently, the "Brussels Effect" has been proposed in reference to the EU's unilateral capacity to regulate products and processes in global markets. Given its specific focus, the Brussels Effect could be more explicity adopted to address the EU Digital Market, including the EU approach to data mining and their storage (Bygrave 2021, Renda 2022). In contrast to the NPE, the Brussels Effect refers to a specific capacity of soft power potentially acquirable by any jurisdiction depending upon the size, behaviour and market forces (Bradford 2020). Here, what moves the spread of EU regulations worldwide is the size and attractiveness of its market. At the same time, the externalisation of its regulatory agenda seems to be a protectionist strategy for its domestic economic goals.

This interpretation of the EU actorness is in line with the regularly announced intention of the European Union to emerge as a "global market rule maker" (European Commission 2007, 2017). Parallel to these aspirations, the EU has steadily emphasised the importance to promote European values for global standards of data privacy laws (European Commission 2010, European Council 2010).

Departing from the extensive debate on the degrees of authority and power that an institution might have in pursuing this goal, in this paper the discussion around NPE and the Brussels Effect contributes to expand our understanding on the EU struggle for legitimacy and leadership in global governance. Here the focus is on the EU capacity in influencing global digital innovation, beyond the traditional realist perspective on great powers and instead consider also the struggle over who governs.

AI and security

Although most of the contemporary debate on AI is related to regulation, innovation and the digital market, the development of AI is tied to the history of warfare and security. The concept of AI builds on Turing's pioneering work "Can Machines Think?" (Turing 1950), with which he developed reflections derived from his effort in designing the so-called "Turing Bomb". This electro-mechanical device was commissioned by the UK Government during the Second World War to decode the German cryptographic language generated by the first-ever designed electro-mechanical device Enigma. Both machines were built to process algorithms able to code and decode data to perform military operations. This early implementation of AI is representative of how the rush to gain computational capacity has been traditionally led by the willingness of countries to strengthen their national security.

Since Turing's work on AI, the latest advancement in the field reflects the recently acquired access to "big data", developments in machine learning approaches, and increased computer processing power. Today, AI consists of a set of elements including data, sensors, algorithms, actuators, and machine learning, that can emulate human cognition in reasoning, learning and autonomously taking actions as a response. These latest progresses in AI have and will continue to have enormous impact on international security. Therefore, due to the digital, physical and political security threats arising from the competition between AI in military applications, private digital innovations and scientific development (Johnson 2019), normative and legal frameworks are seen as crucial to sustain international stability (UNIDIR 2019).

The security dimension of AI has been on the agenda of various international organisations such as the G7, the Organisation for Economic Co-operation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC). However, it is in the context of the UN with the "Convention on Certain Conventional Weapons framework on Lethal Autonomous Weapons Systems" that we can identify one of the first attempts to consider the role of AI in a military context in international cooperation (High Contracting Parties CCW 2019). AI impacts on security in several domains. In the context of cybersecurity, AI can be used for discovering and exploiting vulnerabilities while patching their own ones, therefore, creating a defence against external cyberattacks (Brown 2019, DARPA 2019). AI has attracted concerns in the context of disinformation campaigns (Marsden *et al*. 2020). While AI provides tools for eroding social trust through fast and broad dissemination of credible disinformation and deep fakes (Whyte 2020), machine learning can be applied to detect, analyse and destroy undesired propaganda content. As an economic and financial tool of statecraft, AI can be applied to strengthen counter operations against illicit funds that are the terrorism and Weapons of Mass Destruction runoff (Kirkos *et al*. 2007). In the context of defence, AI systems might also be used in logistics by facilitating the analysis of data to predict various components like equipment maintenance, service member performance and others (Taddeo 2019). Moreover, due to the potential adoption of AI in combat, autonomous systems have been increasingly applied in military systems across the globe with the Lethal Autonomous Weapon Systems (LAWS), capable of independently identifying and destroying a target without human interaction (Haner and Garcia 2019, Horowitz 2019). Due to the accessible nature of AI, also individuals and non-state actors are obtaining the possibility to use the technology (Rassler 2018). Meanwhile, for diplomacy and humanitarian missions, AI could reshape diplomatic practices through its capacity to identify vulnerabilities within personnel and advance communication by lowering language barriers, as well as forecasting political, economic and social trends (Hoadley and Lucas 2018). Finally, AI enhances various daily life operations and other benefits, yet AI systems themselves are faced with threats and therefore need to be secured. Among the possible threats to AI, ENISA (2020) lists malicious acts to ICT infrastructure to steal, alter, or destroy a target; interception of communication without consent; physical attacks; insufficient functioning of assets; and finally, unexpected disruptions.

In addition to the various elements and security applications of AI, there are just as many variances in national security approaches, reports and initiatives (UNIDIR 2019). Today, 48 countries have official national strategies or plans for AI of which 21 are EU Member States[1] (OECD.AI 2021). While every government has the intention to build its AI capabilities and foster economic growth through a safe and ethical environment, the AI application to the military is limited to the acknowledgement that emerging technologies are crucial to integrate into the national security and defence systems. Nonetheless, by boosting their investments for the implementation of AI in their national security strategies, the US, China and Russia are leading the rush to the adoption of AI for military ambitions (Taddeo and Floridi 2018, Boulanin *et al*. 2020, Bendett *et al*. 2021).

The militarisation of AI: US, China and Russia

We may identify four basic strategies, guided by resources and competencies available, that major international actors might adopt (Danilin 2018). Two of them apply to state actors. Technological and innovative superiority is the approach adopted by key global actors through intensified development of emerging technologies through defensive and commercial perspectives. The US has held an indisputable global leadership role, firmly set in its “Artificial Intelligence Strategy” (US Department of Defense 2019). China is also actively engaging in adopting the strategy of technological superiority, notably through the “Made in China 2025” initiative (The State Council of People’s Republic of China 2021) and has been slowly catching up. However, other actors might have limited resources to compete in the race to emerging technology leadership, and therefore might adopt a “tech-deterrence” strategy or support the revision of regional or world order. This typology of strategy is supported either by the development of both defence and commerce, or only defence.

The US perceives military capabilities as essential to the national security agenda that aims to both prevent and respond to conflict. This mirrors the fact that the US has been one of the first countries to carry out an AI-enabled DoD military project “Algorithmic Warfare” also known as “Project Maven” in partnership with Google, aimed to be used for drone footage analysis in operations against non-state actors (Crofts and van Rijswijk 2020). Automated intelligence processing to collect data and identify hostile activity for targeting has been used against ISIS (Deputy Secretary of Defense 2017). The priority of a technologically empowered military is highlighted also by strong investments in research and development (Briscoe and Fairbanks 2020). Political and military leaders of the US have often mentioned a Third Offset deterrence strategy that aims to counter and overcome military modernisation and technological advances made by China and Russia (Lange 2016, Pellerin 2016, Work 2016). This has been emphasised with the establishment of "The Office of Digital and Artificial Intelligence" in February of 2022, which is led by a Chief Officer who oversees DoD's strategy development for data, analytics and AI (US Department of Defense 2022). While the US leads global research and development, different recent reports and indexes demonstrate that other countries are quickly catching up (National Science Board 2020, UNESCO Institute for Statistics 2021).

China is the US' most ambitious and dynamic competitor in AI. In 2017, China released its "Next Generation AI Development Plan" in which AI was described as a "strategic technology" (State Council of China 2017). The document outlines the aim for China to become the leading centre of AI by 2030, based on an innovation-driven strategy for both the civilian and military sectors. As is also mentioned in the strategy, while China has achieved important breakthroughs in various fields of AI innovation and has a considerable number of published scientific papers and innovation patents, there are still various shortcomings that China must address in its quest for domination of AI, such as human capital, key equipment, research and development layout and others (Demchak 2019). Moreover, the plan emphasises the importance of cooperating with internationally leading AI institutes by encouraging domestic enterprises to provide their services to foreigners and to encourage also foreign AI enterprises to establish research centres in China. This tendency can be observed in China's increasing investments in the US AI market (Cheung *et al*. 2016). Vital to achieving the strategy is perceived civil–military integration. There is evident progress and competition among such Chinese technology companies as Baidu, Alibaba and Tencent. Several similar enterprises are increasingly challenging the US in innovation. As for the AI integration within the military, China is following the military concepts of the US. Besides seeking to enhance battlefield decision-making, China is investing in research of autonomous vehicles and AI tools for cyber defence and attack (Kania 2021).

Russia's strategy for AI is heavily based on its application in the defence sector, specifically targeting the roboticisation of the military through various conferences and organisations. The most well-known projects are unmanned ground vehicles capable of carrying machine guns that have a multi-use purpose in combat, intelligence gathering and logistic roles (Horowitz 2018). Additionally, similarly to the US and China, also the Russian military is planning to incorporate AI into other vehicles to make them autonomous and evolve the capability of swarming (Bendett 2017). To counter the US leadership in emerging technologies, Russia is developing Intercontinental Ballistic Missiles (ICBMs) and modernising its nuclear arsenal. Research, development and cooperation with like-minded countries on AI and emerging technologies have been actively taken upon by the Advance Russian Force (Kashin and Raska 2017). While Russia could be perceived as another rival in the pursuit of AI leadership due to its technological developments, as well as policy statements, it lags behind in investments in research and AI. Moreover, until 2019, Russia was the only large country without a strategy for AI development (Petrella *et al*. 2021).

While research in the field usually focuses on Western technological innovation, history on the Chinese and Arab advancement in the field of AI demonstrates that Western superiority over technology is a recent trend. Technology bends to changes, so an environment that seems inoperable, could prove revolutionary in another time (Headrick 2010). Technological superiority, encapsulated in the first-mover advantage in AI, has been and still is the key pillar of US national and military power and global competitiveness, however, China is persistently exercising its strategy of becoming the technological leader. The development of an offensive strategy of innovation, which defines the current competition between the US and China (Kania 2017), typically enhances strategic mobility and global influence. A defensive strategy of innovation on the other hand serves to reassert the autonomy of smaller political entities (Goldman and Andres 1999). Brooks (2017) observes that no state, including the great powers, can remain the leader in military technology unless internationalisation of production is pursued.

The EU, like other actors, views AI from the perspective of global leadership and its strategic and transformative potential (European Commission 2018, High-Level Expert Group on Artificial Intelligence 2019, von der Leyen 2019). However, in the following section, we address how in contrast to other leading actors, notably the US, China and Russia, EU ambitions are not built on solid basis. In particular, what distinguishes the EU is not only the lack of a leading global EU tech industry, which weakens the EU's capacity to lead technological advancements in the field, and causes significant brain drain in the sector (Docquier and Rapoport 2012). It is also very much the nature of the EU itself, and looking at AI from a security perspective, we discuss how the announced ambition to achieve EU Digital Sovereignty is also constrained by the traditional weaknesses of EU defence strategy more broadly.

EU sovereignty over AI

Since the approval of the Treaty on the European Union, EU member states have agreed on the need for a collective commitment to the creation of a coherent defence policy environment (Whitman 1998). However, historically, EU institutions have had a limited reach on defence matters (Zielonka 1998, Nicolaïdis and Howse 2002). While some EU members are seeking greater collaboration and reflection on the role of AI for defence through their national strategies and initiatives, others remain wary of specifying their stance on AI and of incorporating defence use of it in national funding and defence planning. Meanwhile, earlier in 2022, the European Commission released a roadmap on critical technologies which affirms how significant their development is in affecting the global security landscape (European Commission 2022a).

This ambiguous approach to AI in the security sector reflects the existing traditional disagreement about the need for the EU to equip itself with a unique defence strategy shared among member states. Although there have been increasing efforts to work towards the capacity to act autonomously in the military field, liberal theories of international politics do not predict for the EU to have a defence project (Posen 2006). Historically, the goal of the EU has been to improve member states economies to achieve such a level of interdependence that would not permit the development of individual military aspirations. Consequently, technological development and ambitions to establish a supranational technological capability in the EU context has suffered from a lack of unified EU defence among its member states (Citi 2014). The absence of an EU approach to AI is widening the technological capability gaps between EU Member States, and generating inconsistencies in approaching AI across the EU. Although several EU Member States have adopted a national AI strategy, only France has released a specific AI military strategy. With this document, France equiped itself with a guideline on AI-enabled military applications and sets the framework for the creation of various bodies with the role of adopting national military AI (AI Task Force 2019). Moreover, it has been actively promoting its national AI defense and technological superiority goals by establishing such AI-enabled military systems as *nEUROn* – an unmanned combat air vehicle (Barela 2016). Given the intrinsic relationship between AI and security as discussed above, contrary to the US, China and Russia, the lack of this perspective in the development of an EU AI agenda further weakens the EU's ambition to achieve Digital Sovereignty.

More recently, with the establishment of the European Defence Agency (EDA) and Permanent Structured Cooperation in Defence (PESCO), the EU intends to have a greater impact on fostering transnational collaboration. Although cautiously, security and strategic autonomy are set within the frameworks of the EDA. In this context, the former High Representative of the Union for Foreign Affairs and Security Policy Federica Mogherini stressed the primary role of EDA in building a consensus on compliance with international law and the use of AI-enabled weapons (European Defence Agency 2020a). While there has been a certain wariness in releasing a definitive strategy and guidelines, EDA Chief Executive Jiří Šedivý (2021) underpinned that "for the EU to be a credible security provider and a trusted partner in defence [Artificial Intelligence] must be in the centre of our capability development". The EDA has actively been approving various projects involving AI for radar systems (European Parliament 2021a), data collection through simulation training (European Defence Agency 2020b), autonomous drone detectors (European Parliament 2021a) and more. These projects contributing to strategic autonomy are funded by the European Defence Fund (EDF). Out of 60 PESCO projects, Maritime Unmanned Anti-Submarine System (MUSAS) is the only one that directly mentions AI as a part of its agenda. However, while not mentioning AI nor the degree of a system's autonomy, 9 PESCO projects are based upon unmanned systems and their operability.[2]

Despite this latest development, the lack of heterogeneity in defence cooperation is mirrored in low R&D (Soare 2021). While the EU defence investment and expenditure have been constantly growing, only 16.9% of the total investments were spent to fund collaborative defence R&D being "the lowest level of collaborative spending ever measured by EDA" (European Defence Agency 2021, p. 14). The rest has been utilised to procure military equipment and technologies. The EDA has been increasingly working towards developing a joint response on AI capability development but without an officially published plan yet. AI technology and its safety will have an impact on the future developments of capability in the military, industrial and civil sectors. A lack of coordinated security and defence strategy raises the risk of AI capability gaps and issues with interoperability.

Private investments provide little support to improve this situation. European external AI investments reached 4 billion USD in 2016 compared to 12 billion USD in Asia and 23 billion USD in North America (Bughin *et al*. 2017). US private investment in AI companies from 2013–2021 was significantly higher than those of other actors standing at 52 billion USD, while those of China at 17 billion USD, and the EU trailing behind with 6 billion (Zhang *et al*. 2022). American private firms are investing more in AI R&D than European ones – 70 billion EUR and 9 billion EUR respectively (European Investment Bank 2021). Overall, in 2019, the EU is estimated to have spent almost 9 billion EUR in AI investments, and half of them were targeted at skills and capacity building (European Parliament 2021b).

These investments explain the latest picture on the AI Worldwide Ecosystem offered by the EU Joint Research Centre (JRC). In its latest TES Analysis mapping the techno-economic segment of AI, the JRC reports that the US is the leader in the absolute numbers of AI industrial players globally (Samoili *et al*. 2020). The same analysis reports China in second place in the context of total AI players, with the highest number of research institutions in AI, as well as the highest number of patent applications. However, for others the granted number of patents worldwide is instead dominated by North America (Zhang *et al*. 2022). In comparison to US and China, the EU has a stronger position in the research output. However, the EU's lower propensity of AI industrial actors' innovative activities suggests a slower penetration of the technology when compared to the other leading global powers (Samoili *et al*. 2020). Castro *et al*. (2019) have compared talent, research, development, adoption, data and hardware in the context of AI between China, the US and the EU. Overall, their analysis confirms the US as the absolute leader in AI in talent, research, development and hardware, while China is seen as catching up and is the leader in AI adoption and data, and the EU trailing behind with no leading position in any of the categories operationalised.

We can conclude that global investments in AI and the industry of security and defence are dominated by the US and China, with figures that are incomparable to other countries. Massive investments for AI and robotics defence systems are observed also for Israel and Russia. Saudi Arabia, Japan and South Korea on the other side, invest in large-scale procurement of these enabling systems. In the EU context, the long-time awaited Strategic Compass for the EU's security and defence policy (2022) does not offer a clear vision on the future strategic development of AI. Throughout the 64 pages of the document, "artificial intelligence" is mentioned only four times acknowledging it as one of the "critical dependencies" (European External Action Service 2022, p. 48), as well as stating its importance for the improvement of military mobility and innovation (European External Action Service 2022, pp. 31, 47) and operations within the cyber domain (European External Action Service 2022, p. 45).

Finally, given the limited investments *vis-à-vis* other countries, the lack of an EU global leading tech industry, and no support from a coherent defence strategy, the EU seems short of tools to achieve the announced Digital Sovereignty by becoming a global leader in the AI sector. However, as detailed above, since the early implementation of regulatory initiatives targeting its digital market, the EU has triggered standards that not only have protected its citizens but also have imposed an EU view on digital services over the tech industry and third countries (Calderaro *et al*. 2014). We can identify a similar approach also in setting ethical standards in the implementation of AI in the defence industry.

EU Digital Sovereignty: global leadership or normative power?

We have discussed the various challenges that the EU is facing to achieve Digital Sovereignty at the centre of the ambition to develop strategic autonomy. The lack of a Digital Tech industry and other forms of investments coming from the defence sector, prevents the EU from playing a proactive role in the rush to global tech supremacy. In particular, the EU is lagging behind in the domain of AI, while main competitors are constantly moving ahead of the technological boundaries in data mining, algorithms complexity and computational capacity led by the development of quant-computers. In the current scenario, it is difficult to foresee the EU catching up in the nearest future. To the economic, security and geo-political consequences of this situation, we should also consider that in a domain where technology evolves quicker than the capacity to develop norms, policy and regulations, countries in the lead of the current technological developments will also be in a position of advantage to set standards on the use and impact of these technologies (Calderaro and Craig 2020). Consequently, the EU might face future scenarios of declining control and autonomy in this area.

At the same time, we have also discussed how the EU is trying to overcome its dependency of technological dominance by implementing regulations for the protection of its digital market and EU citizens, that have indirectly set an EU view on industry and technology. The emerging voice of the EU in the digital domain is in line with its core values established with Article 3-5, Reform Treaty 2007, clustered around the principles of protection of its citizens and human rights, support to global stability via peace, security, the protection of the Global environment, solidarity and free and fair trade (Cremona 2004, Lucarelli and Manners 2006, Fahey *et al*. 2020).

Similar to the initiatives taken to protect its Digital Market and EU citizens, looking at the relevant implementation of AI in the military sector, the EU has presented a common position on human control over AI-enabled systems at the UN debate on LAWS (Boulanin *et al*. 2020). Following the increased global concern related to the adoption of AI in the defence industry and the consequent use of such weapons (Asaro 2013), in 2017 the UN established a Group of Governmental Experts (UNGGE) on Emerging Technologies in the Area of LAWS. With the goal to identify principles and norms formalised in the context of the UN, due also to the proactive role of EU member states, the UNGGE has identified humanitarian principles in the use of LAWS (Cath *et al*. 2018). In line with this resolution, in early 2021, the European Parliament adopted a text on non-binding guidelines for military and non-military use of AI, placing AI as subject to international public law as is the use of conventional weapons in conflicts. This new resolution identifies the legitimate use of AI in the military sector (Horowitz 2018). Notably, it recognises the utility of AI via the mass processing of health monitoring and environmental risk projection, as well as the possibility for military personnel to stay at a distance in operations in high-risk environments, for mine clearance and defence against drone swarms. This resolution follows a preliminary consensus achieved by the European Parliament in 2018, calling for the ban of LAWS (European Parliament 2018). Although this outcome was not binding, it offered an EU perspective on the adoption of AI in the military realm. Nonetheless, this ban was turned into practice with the launch of the EDF in 2019. On this occasion, the EDF's budget was approved by members of the parliament under the condition that no funds can be allocated on R&D on LAWS, in respect of the 2018 resolution banning their adoption (Boulanin *et al*. 2020).

A similar position concerning ethical application of dual-use technologies was already expressed in 2015, when the EU Parliament adopted the resolution on "Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries" (European Parliament 2015). Two years later, in 2017, the EP Committee for International Trade (INTA) adopted a position promoting the update of the EU regulation concerning the export control of dual-use technologies entitled "Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items" (Committee on International Trade 2017). In May of 2022, the EP adopted recommendations provided by its Special Committee on AI in a Digital Age (AIDA), which highlighted an urgent need for the EU to act "as a global standard-setter in AI" in the light of the AI's potential in human labour, as well as the risk of global standards being developed and sustained by undemocratic actors (European Parliament 2022). We can conclude that where EU Member States' often offer fragmented ideas about what AI is and what role it should play in the defence sector, unity prevailed when developing a collective response to the concerns related to the unethical adoption of AI.

The EU perspective on regulation and protection of individual rights has been seen as hindering aspects of AI development as it makes innovation and data gathering strenuous (Brattberg *et al*. 2020). This criticism could be reverted if the EU implements its regulations with clarity and good guidance (Roberts *et al*. 2021). We have already discussed how Manners (2002) interpreted the EU's capacity to intervene in international affairs by exporting its core values as "normative power". These and subsequent debates on EU external governance and its norms-based approach to foreign policy, have highlighted the capacity of the EU to play a key role in international challenges in line with the EU treaties designed around the idea of protection of civilians and human rights.

In line with the perspectives offered by the NPE and Brussels Effects, that helps us to interpret the EU trying to overcome its lack of leadership in the AI industry and its related security sector, with the promotion of ideas, norms and regulations, the EU is increasingly emphasising the importance of cooperating with other like-minded actors in response to military and security aspects of AI (European Parliament 2022). This is particularly evident in the cyber security domain, where the EU is growing its ambition to play a central role in international cooperation (Calderaro 2021, Barrinha and Christou 2022, Farrand and Carrapico 2022). As a result, the EU is intensifying the establishment of partnerships by expanding its cyber diplomatic approach beyond the realm of security (Marzouki and Calderaro 2022). One of them has been a reinforced cooperation with Brazil on the digital economy through the Digital Economy Dialogue, which ought to discuss also AI (European Commission 2021d). A similar partnership has been reinforced also with Singapore which provides a framework for future cooperation in emerging areas with transformative economic potential, including AI (European Commission 2022b). Finally, the first officialised digital partnership the EU has signed with a partner country was at the EU-Japan Summit in May of 2022 with Japan (European Commission 2022c). In the context of AI, the cooperation between the two actors shall focus on safe and ethical applications of the technology.

As discussed in this article, even if we may observe coherence between EU initiatives taken to gain Digital Sovereignty and protection of core EU values, we have also noted that in the digital domain, the EU has few other options. Contrary to the US' free market-driven development of AI, and the Chinese rush to gain military dominance in the AI sector, without tools to play in this domain, the EU is constrained to adopt an ethical approach to AI. By doing so, it renders distinct its role in the global debate on sustainable digital developments and protect itself from external digital giants. Yet whether it is compatible with the ambition to gain Digital Sovereignty is less evident.

Conclusion

Given that the EU is expanding its competencies in policy fields as diverse as energy, security and development, recent efforts to gain competencies on cross-cutting issues on AI call for developing a better understanding of the relationship between EU digital strategies and strategic positioning in international politics. At the same time, due to its complex political structures and lack of a global leading Digital Tech industry, the EU is facing several challenges in attempting to gain international legitimacy in this domain. With the goal to understand whether and how the EU is developing Digital Sovereignty in the area of AI, this paper has evidenced the significant challenges that the EU is facing in its ambition to successfully gain leadership and strategic autonomy in foreign and security politics specifically. By process tracing EU initiatives in the domain of AI, this paper has, first, discussed how the EU's ambition to gain Digital Sovereignty is currently pursued through regulatory tools aiming at protecting the digital single market. Second, the comparison between the EU's approach and AI strategies of the US and China provides additional evidence on the limited tools that the EU has in pursuing its ambitions of digital sovereignty. Contrary to leading state actors placing their AI industries at the centre of national security, the lack of a coherent EU defence strategy prevents the EU from approaching AI in a similar fashion. However, we have also discussed how, where no agreement could be achieved in identifying a commonly shared tangible approach on AI across EU institutions and its member states, the EU has successfully designed ethical standards in the adoption of AI in its internal market and defence strategy, which does project influence on a global scale.

European Digital Sovereignty comes at a moment where there is no time left as other actors and technologies are rapidly progressing and developing. European Digital Sovereignty is a core part of the aim to advance the strategic autonomy of the EU. It may be a mistake to hinge its success on the adoption of AI capabilities. Not only because of the major and long-term investment this will entail, but also because it would potentially change the fabric of the EU's actorness altogether. Its largely civilian, regulatory and "benevolent" identity is perhaps the reason for its existence in the first place. Equipped with an advanced AI-based security and defence strategy, it will begin to look like a rather different beast.

Notes

1. This list includes Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Egypt, Iceland, India, Japan, Mexico, Morocco, Norway, Peru, Saudi Arabia, Singapore, Japan, Switzerland, Thailand, Tunisia, Turkey, United Arab Emirates, United Kingdom, United States, Urugay, Vietnam. In the EU: Belgium, Croatia, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Portugal, Romania, Slovenia, Spain, Sweden.
2. Amongst which Next Generation Small RPAS (NGSR), EU Beyond Line of Sight (BLOS) Land Battlefield Missile Systems (EU BLOS), European Global RPAS Insertion Architecture System (GLORIA), Integrated Unmanned Ground System (UGS), Maritime (Semi-) Autonomous Systems for Mine Countermeasures (MAS MCM), Medium Size Semi-Autonomous Surface Vehicle (M-SASV), Small Scalable Weapons (SSW), Counter Unmanned Aerial System (C-UAS), and Chemical, Biological, Radiological and Nuclear (CBRN) Surveillance as a Service (CBRN SaaS). The full list of projects and more details are available via: https://pesco.europa.eu/.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Economic and Social Research Council [grant number 520791].

ORCID

Andrea Calderaro http://orcid.org/0000-0002-9518-1099
Stella Blumfelde http://orcid.org/0000-0003-3521-5194

References

AI Task Force. 2019. *Artificial intelligence in support of defence*. Paris: Ministère des Armées.

Archibugi, D., and Mariella, V., 2021. Is a European recovery possible without high-tech public corporations? *Intereconomics*, 56 (3), 160–166.

Asaro, P., 2013. *On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making*. Cambridge: Cambridge University Press.

Azmeh, S., Foster, C., and Echavarri, J., 2020. The international trade regime and the quest for free digital trade. *International studies review*, 22 (3), 671–692.

Barela, S.J., 2016. *Legitimacy and drones: investigating the legality, morality and efficacy of UCAVs*. London: Routledge.

Barrinha, A., and Christou, G., 2022. Speaking sovereignty: the EU in the Cyber Domain. *European Security*, 31 (3), 356–376.

Bellanova, R., Carrapico, H., and Duez, D., 2022. Digital/sovereignty and European security integration. An introduction. *European Security*, 31 (3), 337–355.

Bellanova, R., and Glouftsios, G., 2022. Formatting European security integration through database interoperability. *European security*, 31 (3), 454–474.

Bendett, S. 2017. *Red robots rising*. *Real Clear Defense*.

Bendett, S., *et al*., 2021. *Advanced military technology in Russia*. London: Chatham House.

Boulanin, V., *et al*. 2020. *Responsible military use of artificial intelligence: can the European Union Lead the way in developing best practice?* SIPRI.

Bradford, A., 2020. *The Brussels effect: how the European Union rules the world*. New York: Oxford University Press.

Brattberg, E., Csernatoni, R., and Rugova, V. 2020. *Europe and AI: leading, lagging behind, or carving its own way?* Carnegie Endowmnet for International Peace.

Briscoe, E., and Fairbanks, J., 2020. Artificial scientific intelligence and its impact on national security and foreign policy. *Orbis*, 64 (4), 544–554.

Brooks, S.G., 2017. *Producing security: multinational corporations, globalization, and the changing calculus of conflict*. Princeton, NJ: Princeton University Press.

Brown, M. 2019. Statement by Michael Brown, Director of the Defense Innovation Unit, Before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities Hearing on "Artificial Intelligence Initiatives Within The Defense Innovation Unit". National Security Archive.

Bughin, J., *et al*., 2017. *Artificial intelligence: the next digital frontier?* Mckinsey Global Institute.

Bygrave, L.A., 2021. The 'strasbourg effect' on data protection in light of the 'brussels effect': logic, mechanics and prospects. *Computer law & security review*, 40, 105460.

Calderaro, A., 2021. Diplomacy and responsibilities in the transnational governance of the cyber domain. In: H. Hansen-Magnusson, and A. Vetterlein, eds. *The Routledge handbook of responsibility in world politics* (pp. 394–405). London: Routledge.

Calderaro, A., and Craig, A.J.S., 2020. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third world quarterly*, 41 (6), 917–938.

Calderaro, A., Gollatz, K., and Wagner, B., 2014. *Internet & human rights in foreign policy : comparing narratives in the US and EU internet governance agenda*. Working Paper. Florence: European University Institute.

Castro, D., McLaughlin, M., and Chivot, E. 2019. *Who is winning the AI race: China, the EU or the United States?* Center for Data Innovation.

Cath, C., *et al*., 2018. Artificial intelligence and the 'good society': the US, EU, and UK approach. *Science and engineering ethics*, 24 (2), 505–528.

Cheung, T.M., *et al*. 2016. *Planning for innovation: understanding China's plans for technological, energy, industrial, and defense development*. U.S.- CHINA. ECONOMIC and SECURITY REVIEW COMMISSION. University of California - Institute on Global Conflict and Cooperation.

Citi, M., 2014. Revisiting creeping competences in the EU: the case of security R&D policy. *Journal of European integration*, 36 (2), 135–151.

Committee on International Trade, E.P. 2017. Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast) (COM(2016)0616 – C8-0393/2016–2016/0295(COD)).

Couture, S., and Toupin, S. 2019. What does the notion of "sovereignty" mean when referring to the digital?. *New Media & Society*, 21 (10), 2305–22.

Cremona, M., 2004. The union as a global actor: roles, models and identity. *Common market law review*, 41, 553–573.

Crofts, P., and van Rijswijk, H., 2020. Negotiating 'evil': google, Project Maven and the corporate form. *Law, technology and humans*, 2 (1), 75–90.

Csernatoni, R., 2022. The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European security*, 31 (3), 395–414.

Danilin, I.V., 2018. *Emerging technologies and their impact on international relations and global security*. Washington, DC: Hoover Institution. Text.

DARPA. 2019. Automated Rapid Certification of Software (ARCOS).

Demchak, C.C., 2019. China: determined to dominate cyberspace and AI. *Bulletin of the atomic scientists*, 75 (3), 99–104.

Deputy Secretary of Defense, 2017. *Establishment of an algorithmic warfare cross-functional team (Project Maven)*. Washington, DC: US Department of Defense.

Docquier, F., and Rapoport, H., 2012. Globalization, brain drain, and development. *Journal of economic literature*, 50 (3), 681–730.

ENISA. 2020. *Artificial intelligence cybersecurity challenges*. Report/Study.

ENISA, E.U.A. for C. 2017. Principles and opportunities for a renewed EU cyber security strategy.

European Commission. 2007. The external dimension of the single market review - a single market for 21st century Europe.

European Commission. 2010. A comprehensive approach on personal data protection in the European Union.

European Commission, 2017. *White paper on the future of Europe*. Brussels: European Commission. Text.

European Commission. 2018. Coordinated plan on artificial intelligence.

European Commission. 2020a. Digital Economy and Society Index (DESI) 2019. Country Report: Italy.

European Commission. 2020b. Shaping Europe's digital future.

European Commission. 2021a. Fostering a European approach to artificial intelligence.

European Commission. 2021b. Coordinated plan on artificial intelligence 2021 review, shaping Europe's digital future.

European Commission. 2021c. Europe's digital decade: digital targets for 2030.

European Commission. 2021d. *EU and Brazil to reinforce cooperation ahead of 12th Digital Economy Dialogue*. Shaping Europe's digital future.

European Commission. 2022a. *Roadmap on critical technologies for security and defence*. Strasbourg, Text.

European Commission, 2022b. *Joint statement: EU and Singapore agree to accelerate steps towards a comprehensive digital Partnership*. European Commission.

European Commission. 2022c. *EU-Japan summit: strengthening our partnership*. European Commission.

European Council. 2010. The Stockholm Programme — an open and secure Europe serving and protecting citizens.

European Council. 2013. Conclusions of the European Council of 19/20 December 2013. EUCO 217/13.

European Council. 2020. European Council conclusions, 1-2 October 2020.

European Defence Agency. 2020a. ESA and EDA joint research: advancing into the unknown.

European Defence Agency, 2020b. Artificial intelligence: Joint quest for future defence applications. *European defence matters* (19), 34–37.

European Defence Agency. 2021. Defence Data 2018-2019: Key findings and analysis.

European External Action Service, 2022. *A strategic compass for security and defence: for a European Union that protects its citizens, values and interests and contributes to international peace and security*. Brussels: The European External Action Service.

European External Action Services. 2016. Shared vision, common action: a stronger Europe. A global strategy for the European Union's foreign and security policy.

European Investment Bank. 2021. Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy.

European Parliament. 2012. Human rights in the world and the European Union's policy on the matter including implications for the EU's strategic human rights policy - P7_TA(2012)0126.

European Parliament. 2015. Human rights and technology in third countries.

European Parliament. 2018. Autonomous weapon systems. 2020/2684(RSO).

European Parliament. 2019. Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them.

European Parliament. 2021a. Artificial intelligence: questions of interpretation and application of international law.

European Parliament. 2021b. Artificial intelligence funding under the European Defence Fund.

European Parliament. 2022. Artificial intelligence: MEPs want the EU to be a global standard-setter.

European Parliament and Council of the European Union. 2018. Proposal for a Regulation of the European Parliament and the Council on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. COM/2018/640 final.

Fahey, E., *et al*. 2020. The EU as a Good Global Actor.

Farrand, B., and Carrapico, H., 2022. Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European security*, 31 (3), 435–453.

Flaxman, S., Goel, S., and Rao, J.M., 2016. Filter bubbles, echo chambers, and online news consumption. *Public opinion quarterly*, 80 (S1), 298–320.

Friis, K., and Lysne, O., 2021. Huawei, 5G and security: technological limitations and political responses. *Development and change*, 52 (5), 1174–1195.

Goldman, E.O., and Andres, R.B., 1999. Systemic effects of military innovation and diffusion. *Security studies*, 8 (4), 79–125.

Haner, J., and Garcia, D., 2019. The Artificial Intelligence arms race: trends and world leaders in autonomous weapons development. *Global policy*, 10 (3), 331–337.

Headrick, D.R., 2010. *Power over peoples: technology, environments, and western imperialism, 1400 to the present*. Princeton, NJ: Princeton University Press.

High Contracting Parties CCW. 2019. *Meeting of the high contracting parties to the convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects*. United Nations.

High-Level Expert Group on Artificial Intelligence. 2019. *Policy and investment recommendations for trustworthy AI*. European Commission.

Hintz, A., Dencik, L., and Wahl-Jorgensen, K., 2019. *Digital citizenship in a datafied society*. Cambridge: Polity Press.

Hoadley, D.S., and Lucas, N.J., 2018. *Artificial intelligence and national security*. Washington, DC: US Congress, Congressional Research Service.

Horowitz, M.C., 2018. Artificial Intelligence, international competition, and the balance of power. *Texas national security review*, 1 (3), 22.

Horowitz, M.C., 2019. When speed kills: lethal autonomous weapon systems, deterrence and stability. *Journal of Strategic studies*, 42 (6), 764–788.

Johnson, J., 2019. Artificial intelligence & future warfare: implications for international security. *Defense & security analysis*, 35 (2), 147–169.

Juncker, J.-C. 2018. State of the Union 2018: Annual State of the EU address by President Juncker at the European Parliament.

Kania, E.B. 2017. *Battlefield singularity: artificial intelligence, military revolution, and China's future military power*. Center for a New American Security.

Kania, E.B., 2021. Artificial intelligence in China's revolution in military affairs. *Journal of strategic studies*, 44 (4), 515–542.

Kapczynski, A., 2019. The law of informational capitalism review. *Yale law journal*, 129 (5), 1460–1515.

Kashin, V., and Raska, M. 2017. *Countering the U.S. third offset strategy: Russian perspectives, responses and challenges*. S. Rajaratnam School of International Studies.

Kirkos, E., Spathis, C., and Manolopoulos, Y., 2007. Data mining techniques for the detection of fraudulent financial statements. *Expert systems with applications*, 32 (4), 995–1003.

Lambach, D., and Monsees, L., 2022. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, 31 (3), 377–394.

Lange, K. 2016. 3rd Offset strategy 101: what it is, what the tech focuses are. *The Department of the Navy's Information Technology Magazine*.

Li, H., Yu, L., and He, W., 2019. The impact of GDPR on global technology development. *Journal of global information technology management*, 22 (1), 1–6.

Lucarelli, S., and Manners, I., 2006. *Values and principles in European Union foreign policy*. New York, NY: Routledge.

Manners, I., 2002. Normative power Europe: a contradiction in terms? *JCMS: Journal of common market studies*, 40 (2), 235–258.

Manners, I., and Diez, T., 2007. Reflecting on Normative Power Europe. In: F. Berenskoetter, and M.J. Williams, eds. *Power in world politics*. New York: Routledge, 173–188.

Marsden, C., Meyer, T., and Brown, I., 2020. Platform values and democratic elections: how can the law regulate digital disinformation? *Computer law & security review*, 36, 105373.

Martins, B.O., Lidén, K., and Jumbert, M.G., 2022. Border security and the digitalization of sovereignty: insights from EU borderwork. *European security*, 31 (3), 475–494.

Marzouki, M., and Calderaro A., 2022. *Internet diplomacy: shaping the global politics of cyberspace*. New York, NY: Rowman & Littlefield.

Mazzucato, M., and Perez, C., 2015. Innovation as growth policy: the challenge for Europe. In: J. Fagerberg, S. Laestadius, and B.R. Martin, eds. *The triple challenge for Europe: economic development, climate change, and governance*. Oxford: Oxford University Press, 229–253.

Micklitz, H.-W., *et al*., 2021. *Constitutional challenges in the algorithmic society*. Cambridge: Cambridge University Press.

National Science Board. 2020. The State of U.S. Science and Engineering 2020.

Nicolaïdis, K., and Howse, R., 2002. 'This is my EUtopia … ': narrative as power. *JCMS: Journal of common market studies*, 40 (4), 767–792.

OECD.AI. 2021. Database of national AI policies. Available from: https://www.oecd.ai/dashboards.

Onar, N.F., and Nicolaïdis, K., 2013. The decentring agenda: Europe as a post-colonial power. *Cooperation and conflict*, 48 (2), 283–303.

Pellerin, C. 2016. *Deputy Secretary: third offset strategy Bolsters America's Military Deterrence*. U.S. Department of Defense.

Petrella, S., Miller, C., and Cooper, B., 2021. Russia's artificial intelligence strategy: the role of state-owned firms. *Orbis*, 65 (1), 75–100.

Pohle, J., and Thiel, T., 2020. Digital sovereignty. *Internet policy review*, 9 (4), 1–19.

Posen, B.R., 2006. European Union security and defense policy: response to unipolarity? *Security studies*, 15 (2), 149–186.

Rassler, D. 2018. *The Islamic State and drones: supply, scale, and future threats*. United States Military Academy.

Renda, A., 2022. *Beyond the Brussels effect. leveraging digital regulation for strategic autonomy*. Brussels: Foundation for European Progressive Studies.

Roberts, H., *et al*., 2021. Achieving a 'Good AI society': comparing the aims and progress of the EU and the US. *Science and engineering ethics*, 27 (6).

Samoili, S., *et al*. 2020. TES analysis of AI Worldwide Ecosystem in 2009-2018.

Soare, S.R., 2021. European Defence and AI: game-changer or gradual change? *RSIS commentary*, 51, 4.

State Council of China. 2017. A next generation artificial intelligence development plan.

The State Council of People's Republic of China. 2021. Made in China 2025.

Taddeo, M., 2019. Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and machines*, 29 (2), 187–191.

Taddeo, M., and Floridi, L., 2018. Regulate artificial intelligence to avert cyber arms race. *Nature*, 556 (7701), 296–298.

Timmers, P., 2019. Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and machines*, 29 (4), 635–645.

Turing, A.M., 1950. Computing machinery and intelligence. *Mind*, LIX (236), 433–460.

UNESCO Institute for Statistics. 2021. *Science,technology and innovation*. United Nations.

UNIDIR. 2019. The 2019 innovations dialogue report: digital technologies & international security.

US Department of Defense. 2019. Harnessing AI to advance our security and prosperity.

US Department of Defense. 2022. *DoD Announces Dr. Craig Martell as Chief Digital and Artificial Intelligence Officer*. U.S. Department of Defense.

von der Leyen, U., 2019. *A Union that strives for more: my agenda for Europe : political guidelines for the next European Commission 2019-2024*. Brussels: Publications Office of the European Union.

Whitman, R.G., 1998. *From civilian power to superpower? : the international identity of the European union*. Basingstone: Macmillan.

Whyte, C., 2020. Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of cyber policy*, 5 (2), 199–217.

Woolley, S.C., and Howard, P.N., 2018. *Computational propaganda: political parties, politicians, and political manipulation on social media*. New York: Oxford University Press.

Work, B. 2016. *Remarks by Deputy Secretary work on third offset strategy*. U.S. Department of Defense.

York, J.C., 2021. *Silicon values: the future of free speech under surveillance capitalism*. London: Verso.

Zhang, D., *et al*., 2022. *The AI index 2022 annual report*. Stanford, CA: Stanford Institute for Human-Centered AI.

Zielonka, J., 1998. *Explaining euro-paralysis: why Europe is unable to act in international politics*. Basingstone: Macmillan.

Zuboff, S., 2019. *The age of surveillance capitalism : the fight for a human future at the new frontier of power*. London: Profile Books.