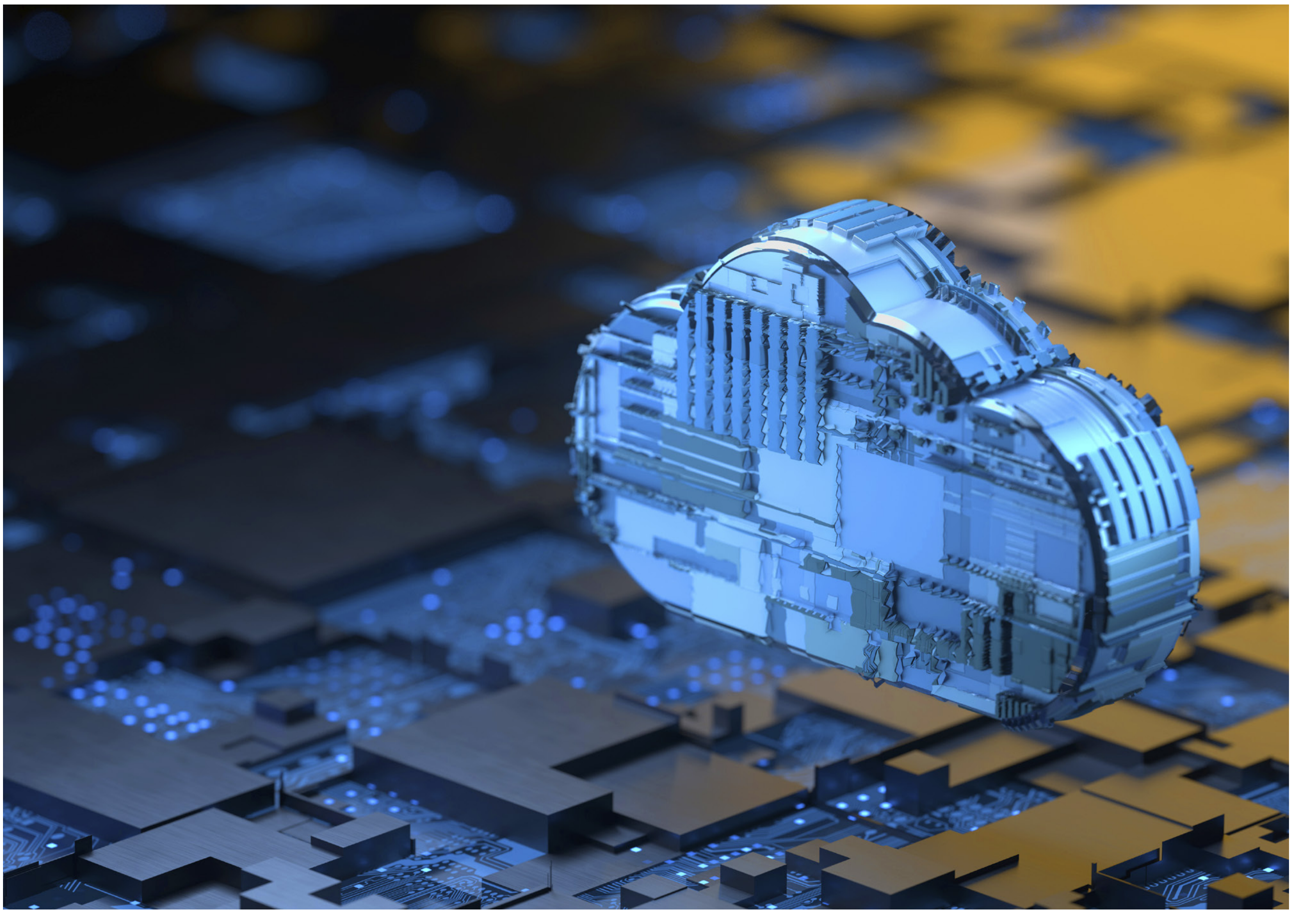
Software-defined Defence: Algorithms at War

Dr Simona R. Soare, Pavneet Singh and Meia Nouwens

February 2023



IISS
The International Institute
for Strategic Studies

Contents

Cover

Cloud computing. (Just_Super via Getty Image)

Executive Summary

Software and artificial intelligence (AI) are critical enablers of modern military operations, lead the evolution towards multi-domain operations, enhance interoperability among allied forces, and support the achievement of information superiority and decision-advantage against adversaries. Much of the functionality and performance offered by military equipment, from the F-35 *Lightning* II fighter jet and the *Patriot* missile-defence system, to the M1 *Abrams* tanks and the French *Griffon*, *Jaguar* and *Serval* armoured vehicles, is already software-defined. As software now drives most of many military platforms' functionality, it is increasingly clear that it is not merely layered on to military hardware. Software is part and parcel of a weapons system.

This report investigates the growing role of defence software and AI/ML (machine learning) in military power now and in the medium term. It focuses on three goals:

- to define software-defined defence. The paper considers software-defined defence to be a fundamental architectural, organisational and operational principle of modern military operations. Software-defined defence entails a new logic for capability development which disaggregates sensors from effectors, software from hardware, and data from specific applications, while connecting them in data-centric, multi-modal, multi-domain, adaptative battle networks;
- to assess ongoing practices and processes in the development of defence software and AI/ML, and identify recurring challenges;
- to explore and assess the ongoing efforts towards software-defined defence in five country case studies – China, France, Germany, the United Kingdom and the United States – and how Sino-American strategic competition is shaping them.

Software-defined defence is based on four foundations. Firstly, a changing relationship between military software and hardware, in which technological progress is faster in software than in hardware, and software-defined functionality of systems increasingly determines operational advantage in information superiority. Secondly, software-defined defence requires a data-centric approach to developing new capabilities and systems-of-systems. Thirdly, it takes a human-centric approach to designing API-enabled end-to-end electronic workflows that enhance human capacity and safety. Finally, software-defined defence regards advanced defence software and AI/ML as a core weapon capability and therefore places emphasis on the software component in early system design, as well as in subsequent upgrades.

The processes used in the development and deployment of advanced defence software and AI/ML remain embedded in decades-old, hardware-driven waterfall capability-development models. Efforts to use agile, iterative and DevSecOps frameworks are incipient across all five countries analysed. However, ongoing initiatives are slow and cumbersome, the causes of which are architectural, organisational and operational. Most advanced defence software is embedded in bespoke hardware, which requires modifications to add new software functionality and improve performance, and defence industries lack enabling digital infrastructure and sufficiently skilled operators. Examples of core operating systems for capability families are slowly beginning to emerge in France, the UK and the US. But more work is needed to move towards a defence-as-a-platform and software-as-a-service-approach.

As Sino-American strategic competition intensifies, with the integration of advanced technologies like AI/ML at its core, China's investment in software-defined defence will narrow the West's military-power advantage. The US is racing to meet this threat and is consistently attempting to accelerate the safe and responsible integration of defence software and AI/ML into its defence capabilities. Similar efforts are only incipient and at smaller scale in France, Germany and the UK. A transatlantic software-defined defence gap has already emerged – one which could still be bridged if Europeans choose to embrace defence software and the digitalisation of defence.

Introduction

Software and artificial-intelligence algorithms are force multipliers, enhance operational art and troop morale, and contribute to victory and defeat on the battlefield. Software not only underpins modern military capabilities but also enables them to collect and analyse data from their environments; communicate with their operators and other systems; control sensors and weapons systems to achieve mission objectives; and protect military personnel and civilians.

Capability development and force-generation processes have not yet accounted for the changing relationship between software and hardware in yielding battlefield effectiveness. Armed forces struggle with the development, deployment and upgrading of modern defence software, particularly artificial intelligence/machine learning (AI/ML). For the United States and its Western allies, 'hardware has always been king and software largely an afterthought'.[1] Flaws in how defence establishments integrate software into hardware-based military platforms generate a high rate of defects in the software. Hardware-dependent embedded software, which is used in most legacy military platforms, is expensive to maintain and difficult to upgrade. Challenges in hardware–software integration and the continuous use of embedded customised software are two of the main drivers of costs and schedule overruns in capability-development programmes. While defence software is recognised as critical to most major weapons systems, for decades it has been 'widely regarded as the highest-risk element in an acquisition', even if software remains the smallest of total programme costs.[2]

This report seeks to conceptualise software-defined defence as a fundamental architectural, organisational and operational principle of modern force generation and military operations, and to explore its key underpinnings. In doing so, it investigates ongoing efforts towards defence software and AI/ML development and uptake in China, France, Germany, the United Kingdom and the US. The research reviews ongoing policy, funding and procedural trends in relation to defence software and AI/ML adoption, and considers specific examples to demonstrate the bottlenecks and obstacles to more effective adoption of modern defence-software solutions. Wherever possible, the report uses examples of military capabilities shared by Western allies to highlight shared challenges related to embracing software-defined defence.

Lengthy capability-development processes designed for hardware-defined platforms in the mid-twentieth century prevent armed forces from exploiting the battlefield potential of software as a weapon and a critical enabler of enhanced manoeuvrability, mass and force protection. This paper argues that software-defined defence requires a new logic in capability development and force generation in which software is the horizontally scaled defence platform enabling the integration of conventional capabilities, AI/ML algorithms and other digital emerging technologies, and the real-time exploitation of very large amounts of data. This means developing military software and hardware in a defence-as-a-platform approach rather than relying on arcane prioritisation between the two. Software-defined defence entails a greater effort on the digital backbone and the software architecture and design of the force to enable accelerated adoption of software and horizontal scaling of software- and hardware-based capabilities.

Amid intensifying Sino-American strategic competition, two dynamics are shaping the technological defence landscape in Europe and North America. Firstly, China's investment in software-defined defence appears to be narrowing the West's military-power advantage and rapidly eroding US and European military technological superiority. Secondly, as the US is accelerating its efforts to adopt advanced technologies in defence, particularly AI/ML, a transatlantic gap in software-defined defence (capability and doctrinal/operational) has emerged. In contrast to France, Germany and the UK, the US has a vision of software-defined defence and, though it faces huge challenges to implementation, it is making efforts to accelerate the development of software-defined capabilities. The transatlantic gap in software-defined defence may still be bridged and interoperability challenges mitigated in the medium term. However, this requires that Europeans more boldly embrace agile and iterative defence software and AI solutions; accelerate the digitalisation of defence; consolidate their defence spending and investment in defence software; and accelerate capability-development processes.

The report is structured in five chapters. Chapter One focuses on identifying what software-defined defence consists of and sets out four key underpinnings of the concept. Chapter Two analyses the challenges in developing and deploying modern defence software, particularly as it pertains to AI-based software solutions. This chapter underlines the data, infrastructure and procedural bottlenecks that limit the pace, scope and scalability of modern defence software across the five case-study countries. Chapter Three offers an interrogation of ongoing defence-innovation efforts in the US and China, and outlines the impact of Sino-American strategic competition on the international system. Chapter Four analyses the efforts towards software-defined defence of three European case-study countries – France, Germany and the UK – and assesses their effectiveness. The Conclusion outlines the implications for European and transatlantic software-defined defence and the strategic risks of falling behind.

1. Conceptual Underpinnings of Software-defined Defence

The existing literature describes software-defined defence through the lens of software that is adaptable and agile in both design and use, defined as the ability to be modified continuously and easily without sacrificing performance or operational utility and without having to modify underlying hardware. It is also multifunctional, effectively sharing the same hardware platform, using virtualisation as the main tool to scale on demand, and encompassing the ability to deliver several capabilities from a single basic design.[3]

This paper conceptualises software-defined defence as a broad architectural, organisational and operational principle of modern defence strategy.[4] The concept is underpinned by the following four defining features, all of which increase speed – particularly the speed of development and the speed of deployment and employment.

1.1. The changing relationship between hardware and software in generating military advantage

Defence software is expanding exponentially every year in terms of the quantity of code and the complexity and autonomy of the tasks performed. In the 1980s, the F-16 fighter jet used thousands of lines of code to actively control flight surfaces without which the aircraft was 'just a $15 million lawn dart'.[5] The F-22 *Raptor* fighter jet, which was introduced in 2005 as the best-in-class capability, deploys 1,700 source lines of code of avionics software, leading senior US Air Force officials to conclude that 'about the only thing you can do with an F-22 without software is take a picture of it'.[6, 7] The fifth-generation F-35 *Lightning* II Joint Strike Fighter introduced a few years later and upgraded in 2022 deploys 24,000 lines of source code of avionics software.[8] That represents an increase by a factor of 14 in the complexity and size of the deployed software between the F-22 and the F-35, without counting the infrastructure code required to allow the fighter jets to communicate and operate together with ground-command stations and other capabilities as well as other applications running on the aircraft's onboard computer. These are not isolated examples. The MQ-9 *Reaper* and RQ-4 *Global Hawk* uninhabited aerial systems (UAS) deploy around 3,500 lines of source code for operational and control software, comparable to the 3,000–5,000 lines of source code deployed on M1 *Abrams* tanks and M2/M3 *Bradley* infantry fighting vehicles. The *Patriot* air-defence system also uses thousands of lines of code to identify, track and intercept incoming targets.

In short, software defines the function, performance and protection parameters of military capabilities alongside the humans who develop and employ them. It is key to upgrading legacy capabilities and building next-generation battle networks. And it has the potential to be more rapidly adaptable than hardware through continuous upgrades without sacrificing performance, utility or readiness. This does not mean military hardware ceases to be important. However, it does signal a changing relationship between software and hardware in delivering military effectiveness and efficiency on and off the battlefield.

The rate of technological progress in software and related hardware components is superior to the rate of technological breakthroughs in conventional military hardware in a three- to five-year period. Because of the rate of technological renewal in software, it can add new or improved functionality in weeks or months, whereas military hardware can only achieve similar impact over decade-long time frames. Recent research shows that dual-use technologies such as mobile telecommunications, LCD displays and Lithium-ion rechargeable batteries matured in less than a decade.[9] On average, this equals one-third to one-fifth of the time other innovations historically needed to mature, even when allowing for variation in the complexity of the technology itself.

Defence digitalisation initiatives such as the Royal Navy's NELSON programme, the US Army's *Project Convergence* and the US Air Force's Advanced Battle Management System could generate new software updates on a two-week cycle, with the potential to reduce this further to daily releases. Though not all these software releases are necessarily new code, they still maintain or improve functionality of mission systems. In other, more software-intensive areas, such as in the electromagnetic spectrum, software release is already possible daily and often hourly if conditions demand it.[10] The US Navy's Task Force 59 demonstrated in 2022 the ability to release software daily and upgrade hardware to an AI-enhanced mesh network within days.[11]

By comparison, mid-life upgrades to military hardware and software almost always come decades apart, usually performed at 12- to 16-year intervals from initial deployment. Delays in the deployment of next-generation capabilities often result in the extension of the operational life of legacy systems by employing defence software or retrofitting them with advanced digital technologies. For example, many legacy programmes, including the *Tomahawk* land-attack cruise missile, the *Patriot* air-defence system, the F-16 *Fighting Falcon* and the F/A-18 *Hornet* fighter jets have had their operational life extended largely due to performance improvements via software upgrades and reconfigurations.[12] Many legacy platforms have recently been retrofitted with new software-defined sensor suites as sensors remain the largest growing area of investment for defence establishments in France, Germany, the UK and the US, as well as the EU and NATO.[13] In some cases, the physical limit of deploying new sensors, displays and gear on military platforms has been reached. However, there are incipient efforts within the defence industry to transition towards more iterative and frequent software upgrades. For example, Saab in Sweden performs software upgrades on military aircraft every two years.

Finally, hardware alone cannot achieve decision-advantage at a time when the real-time exploitation of data and predictive insights promises to define the outer edge of military competitiveness.

Consequently, Western reliance on conventional military hardware (i.e., military platforms) which aggregates sensors and effectors to generate mass and military advantage alone is untenable in the medium and long term without a reorientation towards software-defined defence.

1.2. Data-centric architectures and forces

The more software deployed in defence capabilities, the more defence data it generates. The human capacity to process the exponentially growing volume of data collected by battlefield sensors has already been reached. For example, military sensors collect terabytes of data per second. One CSO French observation satellite produces over 1,000 high-resolution pictures every day, of which human analysts can only process 5% at most.[14] The MQ-1 *Predator* and MQ-9 *Reaper* unmanned aerial vehicles (UAV) generated 14 hours of high-definition video footage in one mission, of which 99% was wasted before *Project Maven*, the US Department of Defense's (DoD) flagship AI intelligence-analysis capability, was implemented in 2017.[15]

To maximise the disruptive impact of software and AI/ML algorithms in defence, a strong data fabric and a mature defence data-management system are needed. Previous IISS research found that all five countries investigated in this paper struggle with maturing their defence data-management systems. The challenges stem from several aspects. These include:

- difficulties in breaking down siloed data structures and fostering enterprise-wide, multidomain data-management systems;
- separating data from systems and applications;
- providing data lakes and shared data for training and development of advanced algorithms;
- ensuring the timely roll-out of enabling infrastructure, such as cloud and edge computing, and reliable and secure wideband communications and networking;
- enabling the use of software factories to accelerate software development;
- consolidating data rights;
- redesigning battle networks to prioritise a cloud-native software-first approach.

In a nutshell, in software-defined defence, military networks are built to accommodate the flexible real-time sharing and exploitation of data across domains rather than data flows having to accommodate network software and hardware protocols, as is the case in network-centric warfare. Enabling military battle networks not just to dynamically share information with each other but to use algorithms that can fuse and process all formats of available data is a fundamental quality and functionality differentiator for software-defined defence.

The ability to share real-time data with different capabilities (and with allies) across different domains is one of the key challenges faced by the US in transitioning to the Joint All-Domain Command and Control (JADC2) concept. The high degree of autonomy that US military services enjoy has already led to the concurrent development of three competing multi-domain command and control (C2) concepts in the air force (the Advanced Battle Management System), the army *(Project Convergence)* and navy *(Project Overmatch)*. However, all three programmes are struggling to identify and deliver capabilities at the moment, often as a result of the inability of US military assets to share data with each other. For example, challenges in data sharing between the F-35, F-22A and KC-46A *Pegasus* aircraft and with ground C2 centres significantly delayed the implementation of the air force's Advanced Battle Management System programme and cost an additional USD600m by the end of 2022, without any capability delivered to the end user.[16] Eventually the only feasible short-term solution was to drop the F-22 from the programme.

This is not a singular case as the US has been struggling with system interoperability between individual weapons platforms and service command, control and communications (C3) systems. It is particularly difficult to enable legacy and newer equipment to smoothly communicate and dynamically share data. Older generations of military platforms were never designed with a digital- and software-first hyperconnectivity framework in mind, and newer systems cannot accommodate these outdated protocols. The F-22A and F-35 fighter jets have incompatible data-link protocols and cannot share information with each other.[17] Similarly, the navy and army C3 systems for ballistic-missile defence cannot share information with each other, and the *Patriot* air-defence system cannot share data with other military assets. During a 2019 NATO demonstration, units of the German 9 Armour Demonstration Brigade could not share data with each other due to the technical incompatibility of IT and C3I systems. Tactical C2 capability was not possible above company level and military personnel resorted instead to unsecure personal mobile phones to transmit reconnaissance data.[18] In addition to an insufficient digital infrastructure, the persistence of legacy software systems which have not been serviced in decades, and the struggle to replace hardware they are embedded in, further complicates the problem.[19]

In 2022, *Project Convergence* demonstrated the ability to share real-time data with other services on a limited basis.[20] During the *Digital Horizon* exercise, the US Navy's Task Force 59 successfully established real-time data exchange between approximately 13 heterogeneous surface and subwater systems via an AI-enhanced mesh network comprising several dozen nodes and cloud-native infrastructure.[21] The exercise demonstrated how cloud-based software-defined capabilities and AI/ML algorithms can enhance situational awareness and military effects at the tactical edge. However, dial-up speed and limitations on data sharing at the tactical edge remain a challenge for most DoD operations.[22] Significant work lies ahead to normalise such data sharing at the national level, let alone at the multinational level within the transatlantic alliance. In October 2022, NATO adopted a 'Data Exploitation Framework Policy' which is an important first step towards a data-centric upgrade of federated networks within the Alliance. However, the framework is limited in relation to NATO's interoperability and operational needs in a software-defined battlefield.[23]

1.3. Software as the core of modular weapon and network design

In 2021, the UK Chief of Defence Staff stated that 'software will be as important as hardware in determining what our Armed Forces will be capable of in the future'.[24] In the US and to a much lesser extent among its European allies, defence software has exponentially increased every decade since the 1970s, as has the complexity and capability of software-defined systems. For example, the percentage of system functions performed by software rose from 8% of the F-4 in 1960 to 45% of the F-16 in 1982 and to 80% of the F-22 in 2000.[25]

Nowadays software is a critical part of modern capability development. The software deployed on the F-35 fighter jet is not just an added layer to the aircraft: it controls the aircraft's aerodynamics, flight and navigation, fire-control and weapons systems, sensor-data fusion and analytics, engine, early-warning and safety systems, and more. In short, software makes the aircraft more manoeuvrable, more lethal, and safer to operate on the battlefield.

By acknowledging that software is an integral part of the lethality of a weapons system or of the defence force more broadly, software-defined defence fosters a new logic for force generation and capability development. In this new logic, software considerations drive the architectural design of weapons systems and of complex military systems-of-systems to 'turn a bunch of disconnected hardware products into an integrated whole that can be operated and managed as a single platform' that centralises direction and decentralises execution of individual tasks, in pursuit of human-defined mission goals, but without the need for manual human intervention.[26]

Enabled by software-defined digital infrastructure, defence software and the underlying defence data-management system become the common horizontally-scaling platform into which military hardware plugs interchangeably to deliver military effects. In software-defined defence a common virtualised software platform can be deployed across multiple military capabilities in the same family and use application programming interfaces (APIs) to enable participation in electronic and often automatic workflows. In the words of Nand Mulchandani and Lt. General (Retd) John Shanahan: 'Just as Apple runs operating systems such as macOS®, iOS® (for iPhones), and iPadOS®, the DOD should envision a day when it has a TankOS®, FighterOS®, and ShipOS® – each running individual hardware systems' that are nevertheless hyperconnected and highly interoperable.[27] A defence-as-a-platform approach, which is integral to software-defined defence, enables individual capabilities to be added or eliminated from the network in real time, and to push software updates and patches to all network components and sub-component applications and systems simultaneously and in real time, without degrading or endangering the overall functionality, performance and availability of military capabilities.

For example, the 2020 upgrade to the US *Aegis* combat system included the development of a Common Core Combat System software application to overcome 'fundamental architectural limitations derived from its initial hardware and software design constraints' and replaced them with an open architecture of 'dynamically loadable real-time tactical combat systems client applications, all potentially executing simultaneously within the software ecosystem'.[28] The F-35 software upgrades in Technology Refresh 3 (TR-3), part of the Block 4 upgrade, envisage the development of similar core combat systems.

Such core software needs to be highly modular and adaptative as well as platform-agnostic and hardware-independent. Notably, it can be deployed on multiple platforms, alongside but isolated from other software, and can collect, share and exploit data from each of them. Adaptable software-defined systems share the same hardware platform with other software and algorithms which run simultaneously and perform distinct tasks. Because they are built by design and used with the purpose of upgrading software-defined functionality iteratively and frequently, such an approach maximises the return on investment on both common hardware (including legacy platforms) and on reusable digital infrastructure.[29]

1.4. A human-defined and human-centric approach by design

Finally, while recognising the centrality of software in defence capabilities, software-defined defence does not advocate replacing humans as the most valuable assets and resources in defence. Software-defined weapon architectures may enable end-to-end electronic workflows which override the need for manual human controls of individual weapons systems, but humans continue to define the requirements and mission goals for the performance and employment of such capabilities on and off the battlefield, and human factors remain a critical consideration for the development of advanced algorithms for defence applications. The key role of human operators in designing the principles of military human–machine teaming and the core consideration given to the human capacity to process machine-generated information in the design of new fighter-jet cockpits demonstrate that software-defined defence does not mean the human is out of the loop. Software-defined defence is premised on enhancing human effectiveness and protection across the full spectrum of defence tasks and therefore needs to encapsulate ethical and legal concerns emerging from this premise.

Human–machine teaming concepts and capabilities such as the ongoing British Army 'Human Machine Teaming' project are examples in which architecture and design decisions drive not just considerations of the functionality of the resulting capability but also technology test, validation, verification and certification approaches, and development and procurement decisions.[30] France, too, is in the process of concluding a multiannual research study on 'Man Machine-Teaming' linked to the Future Combat Air System (FCAS) programme and the technologies that enable it.[31]

Of course, not all defence software is the same. AI/ML technologies in particular remain brittle and require tailored approaches to maturing, testing, verification and certification, as well as new frameworks to ensure their responsible development and use. Likewise, there are different requirements for the development and deployment of staff and payroll software, predictive maintenance software, and target acquisition and fire-control software which need to be accounted for in a software-defined defence approach.

Finally, the inherent logic behind software-defined defence as a human-centric concept is based on transitioning from a world where it takes over 100 operational and logistics staff to operate a MQ-9 *Reaper* UAV to one in which one human can control and direct several military capabilities simultaneously. Collaborative-combat and loyal-wingmen concepts in France, the UK and the US build on the deployment of inhabited capabilities at the core of a battle group comprising dozens or hundreds of unmanned capabilities.

2. A World of Innovation Microscalers

Defence establishments are natural vertical hardware hyperscalers as they continuously seek to increase the number and quality of their defence capabilities. However, they remain microscalers of software-defined defence-innovation solutions as software-defined innovation efforts fail to scale horizontally.

The digitalisation of defence has accelerated over the past three decades, albeit at different speeds, in China, France, Germany, the UK and the US through the exponential increase in the volume and complexity of defence software. However, governments have not adopted competitive business practices for defence software development and procurement.[32] Defence software and AI/ML continue to be developed within waterfall and incremental capability-development frameworks which are not optimised for software's rapid progress.[33]

Efforts to move away from misaligned practices are under way in all the case-study countries. Nevertheless, they are complicated by the sheer scale of change in organisational culture which is required to embrace agile and iterative software-development practices and relinquish the perception of software as risky and an inherent source of weakness. In 2021–22, over half of the DoD's non-classified major capability programmes used agile, iterative and DevSecOps models of software development, although best practices were not fully internalised and consistently applied. Fewer than one in three of these projects delivered new software-defined functionality at intervals of less than six months; fewer than one in ten were releasing software every 2–4 weeks, as recommended by the Defense Science Board; and only one in six was using a software factory in the process.[34] The UK has also begun to experiment with agile and iterative software development on a smaller scale. In October 2022 the Digital Foundry launched a Defence DevSecOps Service (D2B) to enable continuous integration and continuous delivery of software, although this is still struggling to gain traction within the force. Service-level initiatives such as the Royal Navy's data and applications initiative and the Royal Air Force's NEXUS platform build on agile and DevSecOps models to release new software functionality on a continuous basis. The shift towards agile software development remains slower in France and Germany.

2.1. Late adapters to a fundamentally different dual-use technology landscape

Firstly, the structure of the technological landscape has radically changed over the past three decades. Nowadays, private-sector actors lead the technological progress of dual-use software and software-defined hardware.

The gap between governments and the private sector in the pace and scope of technological progress and in the adoption of competitive practices to develop critical advanced technologies is measured in decades.[35] Whereas big tech companies started to exploit data and cloud-computing infrastructure in the early 2000s to generate software-defined hardware such as the iPhone and Tesla cars, or software-defined services and functionality such as Netflix, SpaceX and Uber, most defence establishments (and governments more broadly) are still struggling to adopt such practices.[36] While the tech industry has used digital twins for the better part of the last two decades, the defence industry started to introduce them only a decade ago and is still trying to scale their use.[37]

Governments and traditional defence-industry actors across the world are outspent, outperformed and outinnovated by private-sector actors, big and small. In 2021, big tech companies like Alphabet and Meta invested between USD25–35bn (EUR23–33bn) each in AI R&D, the equivalent of 12–21% of their revenue.[38] This is in addition to similar amounts invested to support the development and maintenance of state-of-the-art digital and cloud infrastructure. Defence unicorns like Palantir and Anduril invested approximately USD560m in AI/ML research and development (R&D) in 2019–20 and could leverage rich venture-capital and private-equity markets to develop new mission systems and defence products.[39]

By comparison, and despite being the top holders of AI/ML patents in the defence sector, in 2021 the leading

European defence primes collectively spent approximately EUR18.5bn (USD21bn) on R&D, on average 3–6% of their budgets, of which AI/ML remains only a fraction.[40, 41] American defence primes invest more in R&D on average than their European counterparts. For example, Lockheed Martin invested USD1.5bn (EUR1.37bn) in R&D in 2021, but AI/ML represents only a small part of its R&D spending.[42]

While commercial and military applications of software and AI/ML have different requirements, private-sector companies in the tech sector push new software releases every two weeks to three months on average. By contrast, software maintenance and development in defence capabilities takes over three years, often focuses on correcting problems in the existing code and algorithms rather than adding new functionality, and comes with a high price tag. For example, one of the largest cost and deadline overruns in the F-35 programme is the cost for the Block 4 *Technology Refresh 3*. This is reportedly over USD4.6bn to 2029, of which USD632m is software- and AI/ML-related.[43] Using an incremental software-development approach, three modernisation increments for the F-22 *Raptor* took twelve years to complete rather than the initially estimated five, during which time projected modernisation costs doubled.[44] Likewise, maintenance and upgrade costs and timelines are not insignificant. Both the F-22A and the F-35 need three weeks' maintenance for every 300 flight hours, during which time the platforms are not available for missions, amounting to over USD22m and USD13.4m respectively in yearly maintenance costs.[45]

Governments cannot sustain or improve their military technological edge by relying solely on government-driven defence-innovation pipelines, or indeed on the traditional defence industry.[46] This is particularly the case in relation to the development and deployment of disruptive defence applications of software and AI/ML, where traditional defence-industry actors no longer define the technological edge, employ the best human talent or access the range of funding required to remain commercially competitive. A 2018 DoD report notes: 'Software development in the commercial world has undergone significant change in the last 15 years, while development of software for defense systems has continued to use techniques developed in the 1970s through the 1990s.'[47] While defence primes are great systems integrators, they have not been as successful at horizontally scaling software-defined architectures and designs in the same way that big tech and other industries have.

For cost-structure and other industry reasons, the defence industry lacks strong incentives to move away from decades-long incremental capability-development models.[48] This often happens with the complicity of defence establishments, reinforcing a vicious cycle in which neither the manufacturers nor the clients have any incentive to foster more agile development and adoption. This also reinforces a pattern of long-term and costly upgrades to defence software, rather than adopting a software-as-a-service approach of continuous integration and continuous delivery. For example, vendor lock-in for mission-system computers for the AV-8 *Harrier*, F/A-18 *Hornet* and EA-18G *Growler* aircraft led to three software releases in the space of ten years from the sole designer, developer and manufacturer of the capability. This does not mean the role of the conventional defence industry is diminished – that is certainly not the case in terms of systems integration. New market dynamics of closer cooperation between defence primes and non-traditional defence start-ups and mid-sized companies are emerging with the potential to impact software development and delivery schedules. Examples include recent Helsing partnerships with Rheinmetall and MBDA, Thales' partnership with Atos, Palantir's partnership with Microsoft, and Atos' partnership with Amazon Web Services.[49, 50, 51]

2.2. Defence software and AI/ML investment

Government investment in defence applications of AI/ML technologies as well as the digitalisation of defence has nominally grown steadily over the past decade. Most AI/ML funding continues to be allocated in defence R&D budgets, but assessing real governmental investment remains very challenging because of the opaque nature of national R&D budgets and the lack of clear budget lines for software and digital capability within major capability-development programmes. The data included in this paper assesses government budgetary pledges towards AI/ML rather than actual AI/ML-allocated defence funding, as insufficient public data on the latter makes a credible estimate challenging.

This limitation creates challenges in assessing the veracity of average annual AI/ML defence expenditure, especially for countries like the UK, France and Germany which have announced multi-annual budgets for this technology. In such cases most AI/ML funds are in fact backloaded by virtue of the growing number and scope of relevant funded initiatives over time, creating the perception of year-on-year budgetary rises in defence investment.

Country comparison of AI/ML defence expenditure is further complicated by the different national taxonomies of AI/ML and the variable national costs of AI/ML innovation in this technology stack. Investment pledges are also affected by the current high inflation rates across the five case-study countries.

The US and China are the largest spenders on defence software and AI/ML by a large margin in comparison to European countries, as depicted in Table 1. Nominally, the US defence budget for fiscal year (FY) 2023 includes approximately USD875m for AI/ML and USD3.98bn on software and digital-modernisation pilot programmes mandated by Congress.[52] AI/ML expenditure represents 0.67% of the DoD's Research, Development, Test and Evaluation (RDT&E) budget, which in FY23 has seen 'the largest increase in any single account within the defence budget'.[53] This includes a USD200m Artificial Intelligence and Development Fund created by the DoD in 2021 to improve tactical AI at combatant commands. According to the DoD Comptroller's Office, in FY23 the US will spend an additional USD1.62bn on AI/ML, representing approximately 3% of the DoD's USD57.9bn non-classified budget for IT and cyberspace activities, of which most funds go towards DoD enterprise software.

Nevertheless, there is reason to suspect the DoD's AI/ML budgets are understated. In 2020, Bloomberg Government estimated that the total DoD expenditure on AI/ML technologies amounted to USD4bn and projected it to increase to USD5.2bn in 2022. A 2020 CSET report assessed DoD AI/ML expenditure between FY2018–FY2020 at USD11.6bn, amounting to USD3.9bn annual expenditure.[54] Calculating conservatively, the estimated defence-wide value of DoD projects including AI/ML in FY23 is USD29.07bn, nearly double the enacted budget for similar projects in FY22.[55] However, these costs often include AI/ML as well as other dependent hardware, network and human-labour costs. Estimated costs for AI/ML software development alone range from USD410,000 for automatic test systems to USD1.3m for AI/ML-enabled tactical intelligence collection and processing on the MV-Osprey platform.[56] Moreover, Govini estimates that overall AI/ML and autonomy investment across the DoD, military services and other US defence agencies may be as high as 50bn.[57]

Between 2017 and 2021, US defence investment in emerging technologies nearly doubled from USD60.7bn to USD117.2bn. Recent Govini data suggests this exponential increase was driven by the response to the COVID-19 pandemic: the largest budgetary increase was in biotechnology, consistent with a response to the pandemic. However, AI/ML investment remained positive across all the sub-stacks, even when adjusted for inflation. The growth in US defence investment was particularly notable in the fields of decision science (USD3.1bn, with a 25.9% year-on-year budget increase), natural language

Table 1: **National defence spending and pledged AI/ML defence expenditure in China, France, Germany, the UK and the US***

Country	2022 defence spending (USDbn, current)	2022 defence R&D spending (USDbn, current)	Pledged annual defence R&D spending on AI/ML, 2018–22 (USDbn, current)
China**	242.4	N/A	e0.3–1.6
France	54.4	6.6	0.1
Germany	53.4	1.7	0.2
UK***	71.4	2.2	e0.4–0.5
US****	766.6	114.7	0.8–e2.5

*Data for China's 2022 defence R&D spending on AI/ML is not available; estimated expenditure reflects 2020 data presented in Ryan Fedasiuk, Jennifer Melot and Ben Murphy, 'Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence', Center for Security and Emerging Technology, October 2021. The defence AI/ML expenditure of all other case-study countries is from 2022, the latest available defence data. **China's R&D defence expenditure is not public and cannot be estimated with confidence. Data on Chinese defence AI/ML spending for 2022 is not available. ***The UK MoD has not made any public pledges for defence AI/ML spending. The figure in the table is an estimate based on defence R&D AI projects, Defence Digital annual spending and investments from other innovation funds. ****Estimated US expenditure calculated based on Office of the Under Secretary of Defense (Comptroller), 'RDT&E Programs (R-1)', April 2022'.
Note: e = estimated figure.
Source: IISS, 2023

processing (USD711m; 19.7% year on year) and machine learning (USD2bn; 15.3% year on year). Data-at-scale and computer vision were the areas with the smallest year-on-year budget increases. However, both categories benefitted from significant investment, at USD40.2 and USD2.3bn respectively.[58] Encouragingly, other supportive technologies, including data-visualisation interfaces and advanced communications, also registered moderate budget increases over this period.

In 2017, China pledged to invest CNY1trn (USD148.6bn) by 2030 to become a leading country in AI/ML technologies. This amounts to roughly CNY76.9bn (USD11.4bn) in annual investments across the civilian and military domains. Under Beijing's Military-Civil Fusion (MCF) policy, efforts are underway for the People's Liberation Army (PLA) to better and more rapidly access and adopt cutting-edge AI technologies from the private sector. In 2018, China's estimated civilian AI/ML R&D investment was a maximum of CNY39bn (USD5.7bn). Beijing does not publish a defence budget line for AI/ML. However, available assessments of its defence AI/ML investments range between approximately CNY1.8bn (USD300m) and CNY19bn (USD2.7bn).[59] In addition, other data suggests Chinese defence expenditure on AI/ML was as high as 1.9% of the PLA's procurement budget in 2020.[60] In 2021, Beijing pledged a 10.6% increase in its defence basic research and a 7% annual increase in its defence R&D spending by 2026. Western sources assess that China's defence AI/ML expenditure is in the low billions and 'on the same order of magnitude as [the] US'.[61]

While China's resources for AI/ML are very large, so is the cost of innovation. Inefficiencies in the coordination of military–civil fusion between local and central authorities raise the cost of innovation, causing delays in achieving overall PLA defence-digitalisation goals.[62] These internal weaknesses are often obscured, but they partially offset the perceived advantage the Chinese regime has in mobilising and directing resources or accessing private-sector technologies for defence application and exploitation. The PLA's non-classified AI/ML procurement contract costs in 2020 ranged from CNY9,000 (USD1,330) for an intelligent sound-and-light alarm detection system) to CNY21m (USD3.1m) for an intelligent UAV data-access and -management platform, with AI/ML contract costs averaging around CNY1.7m (USD251,000).[63]

In comparison, France, Germany and the UK invest only a fraction of Sino-American budgets in AI/ML R&D. In 2021, the British government pledged a GBP6.6bn (USD8.66bn) increase in investment in defence R&D, amounting on average to GBP1.65bn (USD 2.16bn) additional annual investments between 2019 and 2023.[64] In 2020, the government pledged an additional GBP100m (USD122.2m) increase in defence R&D, in addition to the GBP800m (USD963.3m) in the Defence Innovation Fund over the period 2018–28.[65] Moreover, the government pledged a 33% increase in the overall R&D budget from GBP15bn (USD18.3bn) to GBP20bn (USD24.4bn) between 2021 and 2024.

The Ministry of Defence also set aside an additional GBP4.4bn (USD5.38bn) from 2025–26 onwards to exploit advanced technologies, including AI/ML applications.[66] The UK will spend an estimated GBP24.9bn (USD30.4bn) on digital, cyber and ICT between 2018 and 2028, with most individual software-as-a-service contracts in 2022 averaging in the mid-five-to-six figures. AI/ML RDT&E and procurement contracts average in the low seven-figure range, as evidenced by the cost of navy's Intelligent Ship phase 3, the army's Human Machine Teaming project phase 1, the marines' mine-hunting capability autonomy-integrator system, and the project *TALOS* AI-enabled base defence system (i.e., GBP2–3.8m/USD2.4–4.58m). Big data analytics contracts, such as the MoD's SOCIETAS project focusing on electronic warfare mission data and enterprise business software contracts, are generally more expensive (for example, GBP98–150m/USD118–162m) in 2022.[67] The MoD's estimated digital, cyber and ICT expenditure is GBP24.9bn (USD29.5bn) from 2018–28. The Ministry of Defence's estimated annual spend on digital in 2021–22 rose to GBP4.4bn (USD5.3bn), of which 47% was consumed by the upgrade and replacement of three core enterprise digital systems.[68] Cost and deadline overruns in all key digital-capability projects were significant. For example, the estimated cost overrun for the Next Generation Core Network programme is GBP600m (USD733.2m).[69]

In 2021–22 the UK invested GBP1.83bn (USD2.24bn) in defence R&D, marking a GBP800m (USD939.7m) year-on-year increase from 2020, which supports our finding that these budgets are backloaded.[70] However, budget allocations and actual annual appropriations continue to pose challenges. For example, Defence Digital's budget of GBP1.84bn (USD2.26bn) over ten years included a GBP658m (USD804m) allocation in the first four years. However, only GBP410m (USD501m) was available at the launch of the digital-transformation agenda, leading to postponement in key capability projects.[71] Moreover, official ministry sources forecast that digital-defence expenses would be GBP1.4–3.7bn (USD1.71–4.5bn) over the coming decade.[72]

Comparable investment was announced in France in 2018. President Macron pledged a EUR1.5bn (USD1.63bn) investment in AI/ML between 2018 and 2022, notably an average EUR300m (USD327m) annual investment split between defence and civilian R&D.[73] In 2021, France spent EUR6.6bn (USD7.2bn) on defence R&D, with EUR901m (USD982m) allocated to support actions for innovation and emerging technologies. Of the allocated funds, only EUR884m (USD963m) was actually spent on specific projects. In 2022 the ministry underspend on innovation and emerging technologies was even larger, with over EUR100m (USD109m) going unused.[74] These allocations indicate a trend towards incremental increases in French investment in technological innovation in relation to data, AI and other technologies despite limitations in institutional capacity to rapidly absorb increased funding.

However, the share of these budgets represented by defence investments in AI is relatively small, with most funding going to large programmes of record. The 2019–25 military spending plan *(loi de la programmation militaire)* allocated over EUR705m (USD768m) for AI/ML defence R&D/research and technology (R&T), amounting to over EUR100m (USD109m) annually.[75] However, there is emerging evidence to suggest the budgets are backloaded. In 2020, the French Ministry of the Armed Forces spent EUR61m (USD66.4m) on AI/ML applications through its R&T budget, representing 5.8% of the overall R&T budget, of which EUR21m (34.4%) was spent on the *ARTEMIS (Architecture de traitement et d'exploitation massive de l'information multi-sources et d'Intelligence artificielle)* project discussed later in this paper.[76] Furthermore, official data suggests funding for dual-use technologies in defence R&D is steadily declining, despite a policy prioritising the uptake of advanced technologies.[77]

The rising costs of ongoing large-ticket projects like *ARTEMIS* and *SCORPION (Synergie du contact renforcée par la polyvalence et l'infovalorisation)* support the assumption of growing French defence AI/ML spending. So far *ARTEMIS*'s budget was EUR6m (USD6.5m) in phase one and EUR50m (USD54.4m) in phase two, with an estimated EUR300m (USD327m) under discussion for the newly launched phase three.[78] In October 2022, the Ministry of the Armed Forces awarded a contract as part of project *TORNADE (Traitement Optique et Radar par Neurones Artificiels via Détecteur)*, intended to provide the armed forces with an AI-enabled analysis of electromagnetic-spectrum data, to French company Preligens (formerly Earthcube) for EUR240m (USD259m).[79]

The Ministry of the Armed Forces announced an EUR8bn (USD8.63bn) R&D budget in 2023, which includes EUR1bn (USD1.08bn) in innovation funding. In addition, spending on defence software and AI/ML could also be supported from the ministry's EUR702m (USD757.7m) space funding, its EUR467m (USD504.1m) funding for information-warfare systems, and its EUR5bn (USD5.40bn) maintenance budget.[80] Since 2018, the Defence Innovation Agency has been managing a portfolio of 454 projects with committed investments of EUR1.4bn, though there is no public data suggesting that any of these projects have successfully transitioned to the armed forces at the time of writing.[81] There is also no publicly available data to ascertain the value of AI investments as part of the ministry's much larger procurement budgets. For example, it is unclear what share of project *SCORPION*'s EUR10bn (USD10.9bn) budget is dedicated to software and AI development.

Unlike Germany and the UK, which rely on a multinational technological defence base and are often happy to procure off-the-shelf tailored solutions, France's relationship with its national industrial base is far more organic. The defence ministry's 2017 and 2020 IT, cloud and data-management direct-award contracts with Microsoft were internally contested because of a perceived loss of data and digital autonomy. To maintain analytical and decision-making autonomy, Paris has often taken steps to ensure national overwhip over key advanced software providers. For example, in 2020, when In-Q-Tel showed interest in buying the French tech company Preligens (formerly Earthcube), two French-based defence private-equity funds, Definvest and Ace Tikehau, helped raise over EUR20m (USD21.6m) to keep the company's French ownership.[82]

Finally, Germany is the only case-study country to spend less than 2% of its GDP on defence.[83] Berlin pledged EUR5bn (USD5.44bn) between 2020–25 for the implementation of its national AI strategy, which notoriously excludes defence. In addition, Berlin reportedly allocated EUR2bn (USD2.18bn) to defence AI/ML R&D between 2019 and 2029, amounting to an average EUR200m (USD218m) annual investment. However, the lack of transparency around the structure of the Federal Ministry of Defence's R&D budget makes it difficult to ascertain the exact amounts allocated and spent on digitalisation and AI/ML respectively. For example, the 2021 R&D budget amounted to EUR1.55bn (USD1.69bn), within which there is a generic R&D/T budget of over EUR1bn (USD1.09bn); AI/ML applications and defence software are only two of the technologies which could be funded from this.[84] In 2022, Germany's defence R&D budget amounted to EUR1.6bn (USD1.74bn), while in 2023 the budget is expected to rise to EUR1.74bn (USD1.9bn), representing 4.51% of total German defence spending, with approximately EUR1bn (USD1.09bn) for other R&T activities, including digitalisation and AI/ML. Discouragingly, the funding for key emerging technologies has decreased steadily from EUR40m (USD43.6m) in 2021 to an estimated EUR24.65m (USD26.9m) in 2023, suggesting the federal government's investment in AI/ML and other digital technologies may also be under pressure.[85]

Due to the opacity of R&D budgets, it is difficult to accurately assess the ministry's annual spend on AI or to establish the share of procurement budgets dedicated to digitalisation and AI. The Cyber Innovation Hub's EUR10m (USD10.8m) annual budget funds 70 projects (including overhead costs), averaging at just over EUR140,000 (USD151,000) per project. The cost structure for the project to retrofit land vehicles with a newly designed digital C2 system is estimated to be worth several billion euros, with no clarity around the cost of software development versus the cost of upgrading proprietary hardware on thousands of German Bundeswehr inventories.[86] The same applies to the modernisation of the Bundeswehr's Digital Land-based Operations (D-LBO) and Tactical Edge Networking (TEN) systems, as well as to the more recently launched Mission Enabling Service Bundeswehr (MESBw), which seeks to provide modular and modern IT systems services and modernised C2 systems for all domains for both stationary and deployed forces.[87]

In 2022, following Russia's invasion of Ukraine, German Chancellor Olaf Schultz announced that in addition to increasing defence spending to 2% of GDP, Berlin would invest a further EUR100bn (USD109bn) in defence over the next decade as part of a special one-off Defence Fund. This included a EUR21bn (USD22.8bn) investment plan for digitalisation of defence, including the modernisation of telecommunications, IT and digital infrastructure across the German armed forces. The ministry reportedly only planned to invest approximately EUR421m (USD463m) in defence applications of AI/ML.[88]

France, the UK and the US have set up several government-backed defence-investment funds to encourage and support the development and maturation of emerging technologies, including AI/ML in defence applications. Recent examples of DoD-backed venture-capital funds are the air force's AFVentures, a division of its in-house innovation platform AFWERX, which invested over USD710m in new technologies between 2018 and 2020.[89] In the UK, the Ministry of Defence established the Royal Navy's Defence Transformation Fund with a GBP75m (USD91.6m) budget; the National Security Strategic Investment Fund, which comprises seven independent venture-capital funds, each with investment of over GBP10m (USD12.2m); and the army's Transformation Fund, with an initial investment of approximately GBP66m (USD80.7m).

Similarly, in 2017 France launched the Definvest venture-capital fund operated by the French investment bank Bpifrance. The fund benefitted from a EUR50m (USD54.5m) initial investment and the ambition is to double this amount in five years. By the end of 2020, Definvest had invested over EUR18m (USD19.6m) in nine French tech start-ups, and by 2022 official French sources claimed the fund had doubled its investments to EUR100m (USD109m).[90, 91] In 2021, the Ministry of the Armed Forces launched another investment fund, the DefInnov fund, with an initial investment of EUR200m (USD218m).[92] From 2020–22 the Definvest fund undertook deals valued between EUR500,000 (USD545,000) and EUR5m (USD54m).[93]

Such award levels are significantly larger than the grants and awards that British, French and German defence agencies offer for R&D competitions in AI/ML and more aligned with those in the US, which range between USD275,000 and USD10.4m.[94] In France, Germany and the UK – as well as within the EU and NATO – such grants and awards generally range between EUR50,000 (USD54,500) in the first round of competition and EUR150–250,000 (USD163–275,000) in subsequent rounds.[95] Meanwhile, UKRI is Europe's largest investor in emerging and disruptive technologies, including AI/ML for defence and civilian applications, followed by a margin by the European Commission.[96]

2.3. Not agile enough

Scholars and defence analysts in the US and Europe agree that software development and acquisition remain a huge challenge for defence establishments in the US and, to an even greater degree, in Europe.[97] Outdated procurement practices are generally considered one of the main obstacles to software-driven defence innovation, but they are not the only one.

This report interrogates major conventional weapons capability-development projects from France, Germany, the UK and the US between 2020 and 2022 with a view to assessing (a) what capability-development models are primarily used to develop and adopt defence software; (b) how defence software is integrated into complex multiannual capability-development programmes; (c) what proportion of funding is allocated to defence software and AI/ML systems within complex capability-development programmes; and (d) how defence software is generally rated in terms of risk to the prospective project.

Firstly, traditional waterfall models remain the principal capability-development model for the development and adoption of defence software and AI/ML across France, Germany, the UK and the US. However, in the US and the UK, new agile and iterative software-development models are beginning to be incorporated in capability development by virtue of new software-dedicated acquisition pathways. In the US, nearly half of major capability programmes originating in the army, air force and navy currently incorporate at least one agile or iterative model for software development – albeit they often do so within the framework of waterfall capability-development models.[98] Moreover, enabling data and digital infrastructure is often a cascading rather than a parallel process, delaying the software's impact through rapid exploitation by the end user.

For example, Boeing segmented software development for the US KC-46A *Tanker* programme into small iterative development increments which are part of the programme's overall waterfall development model.[99] As such, it accelerated the upgrade- and software-release timetable considerably in comparison to a traditional waterfall model. By contrast, according to the US Governmental Accountability Office, the challenges encountered by the F-35 programme were largely to do with the late development and testing (or lack of testing) of the software suites.

The findings from the US programmes are consistent with capability-development models used in the UK and France, but not Germany. Indeed, when it is not procuring capabilities off-the-shelf as the F-35 fighter jet and adding a particular configuration to meet German capability requirements, Germany remains the only European country to preponderantly use waterfall capability-development models for software development. New structures like the Cyber Innovation Hub have developed AI/ML-enabled travel and health applications for the armed forces in six months or less.[100] However, lengthy German defence procurement and certification processes would likely preclude warfighting applications from being fielded as rapidly.

This is partly an organisational-culture problem related to the inertia of entrenched models and procedures. However, it also stems from a leadership-culture problem in these countries. Agile development and DevSecOps require a close interaction between developers, end users and procurement stakeholders in which end users iteratively assess and adjust the functionality of tested software to meet their needs and requirements. However, political and military leadership remain fundamentally uncomfortable with this procedure, whereby soldiers are actively involved in deciding the functionality of future or upgraded legacy capabilities.

Secondly, defence software and AI/ML solutions are generally integrated in the later stages of capability projects as customised or embedded software which is frequently linked to bespoke hardware.[101] Customised software is code that is developed specifically for a set of military requirements; it is platform and hardware dependent, in opposition to adapted software or commercial software which can run on commercial and modified military hardware. Modified software is commercially available code tailored to the needs of the military end user and is often platform dependent, whereas commercial software is purchased off-the-shelf and directly deployed on license or otherwise.

Because of proprietary limitations in both software and hardware, such defence software is difficult and very costly to upgrade, leading to longer gaps between software releases and high costs for maintenance and upgrade. For example, in the US as well as among European countries, the integration of hardware and software is still perceived as the highest risk when integrating software components in major defence capability-development projects. Therefore, instead of 6- to 12-month software release cycles, capabilities incorporating customised software and hardware suites often need to wait for mid-life upgrades 10–15 years after they were operationally deployed. Nevertheless, customised software, including AI algorithms, represent most of the defence software under development in major conventional capability-development programmes in France, Germany, the UK and the US. Key metrics for budgeting and assessment of such customised defence software revolve around measuring source lines of code. The latter fits a vertical scaling model that remains prevalent within defence establishments rather than a horizontal scaling logic for defence software.

For example, the airborne warning and control system (AWACS) aircraft is being upgraded to migrate 'the hardware and software architectures and applications on the E-3 AWACS aircraft from legacy proprietary systems to new open architecture hardware and software'.[102] The use of hardware-dependent customised software limited the remit of the upgrade itself, resulting in reduced operational capabilities by comparison to the legacy Block 30/35 aircraft deployed two decades ago. Like the F-35, the Franco-German FCAS programme, which was reconfirmed in late 2022, is currently developing a suite of AI-enabled situational-awareness, pilot-health-monitoring, and real-time data-fusion and -analysis systems. However, it is unclear whether such code will be built on an open platform, given the challenges around intellectual property inherent in the multinational negotiations over the programme.

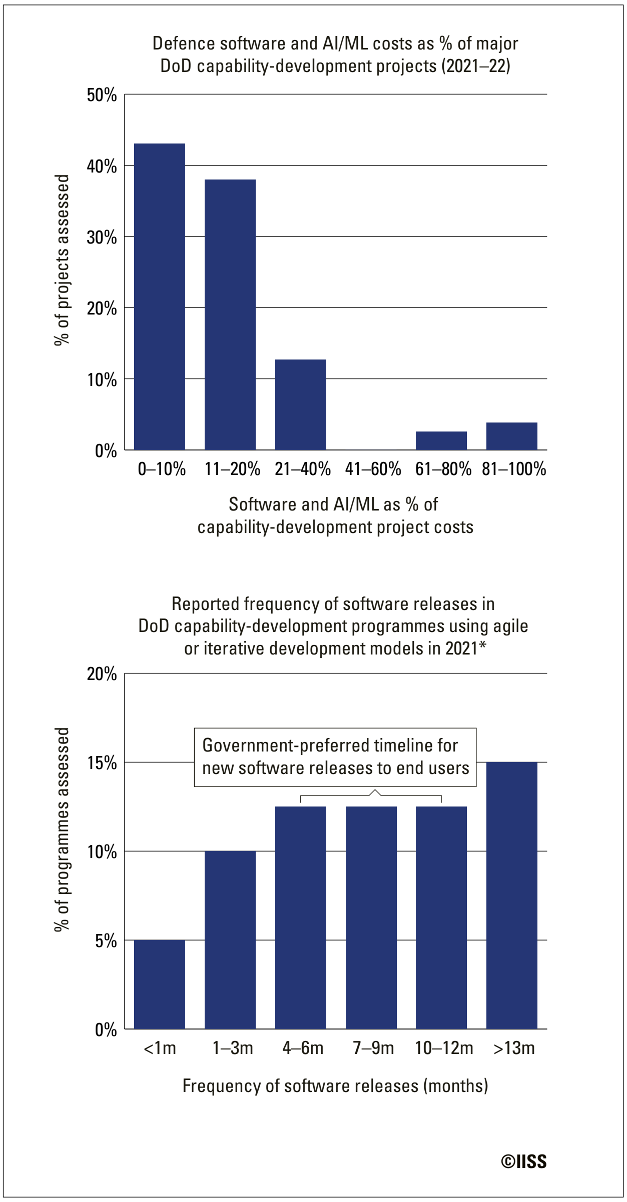
Thirdly, assessing the costs of software and AI/ML within larger capability-development projects is challenging. Defence software is frequently the smallest part of a capability project budget despite having a huge impact on the functionality and performance of the overall capability throughout its life cycle. The weighted average of software costs within broader capability-development projects in the US is 20.7% for 2021–22, while most projects include a 10–20% software cost share. However, in major conventional military platforms such as aircraft, ship or helicopter programmes, software stands at only 1–2% of overall programme costs. For example, defence software within the US Army's armoured multi-purpose vehicle (AMPV) programme accounts for only 2% of total costs, and 90% of those are customised software.[103] In 2021–22, only 3.8% of 79 major defence-capability projects investigated by the US Government Accountability Office (GAO) had a software component of 80–100% of project costs. In 81% of capability projects, software accounted for 20% of project costs or less, and in 43% of projects it accounted for 10% of project costs or less. Nearly half of the projects investigated included 100% customised software requirements. Most of the programmes reviewed included software costs of USD51–670m. However, software-intensive programmes such as the Next Generation Operational Control System might spend between USD6.9bn on software systems, though it is unclear how much is represented by AI/ML costs.[104] The programme plans software releases at intervals of 13 months or longer. Of the software used, the programme will deploy 37% commercially available software, with 42% being customised software and the remaining 21% modified commercial software.[105]

In FY22, the number of rapid-prototyping software-intensive programmes in which software accounts for 40–80% of the programme costs has increased in comparison to FY20 and FY21. This is a testament to the incremental adoption of agile, iterative or mixed capability-development models by the DoD and the military services. However, much work remains to be done. The share of customised software remains high even across agile development practices – around a minimum of 40–50% of the total software developed. Moreover, software release times remain on average longer than the Defense Science Board-recommended 3–6 months or less. The trend towards an acceleration of defence-software releases in capability development is not necessarily clear-cut. US official defence data reveals only 25% of all capability-development projects release new software in three months or less. The same data reveals that the same proportion of projects still take 13 months or more to release software.[106]

Finally, defence software is consistently perceived as one of the biggest critical risks to capability projects. In the US, a recent official estimate suggests over 60% of capability-development programmes classify the risk associated with defence software to be moderate or critical.[107] This is partly explained by failures to design software at the beginning of the capability design and to iteratively develop and test software suites. It is also explained by consistent failures to adequately assess how critical software-defined capabilities will be to the functioning of the capability itself, particularly for more hardware-intensive conventional programmes, to adequately assess the maturity level of desired software technologies and whether they can be matured in time for delivery timelines.[108]

In short, the overarching logic of software-defined defence across all case-study countries analysed remains tied to vertical rather than horizontal scaling. As a result, defence establishments in France, Germany, the UK and the US, and to a lesser extent China, are proliferating new initiatives, structures, agencies and programmes in the development of modern defence software and AI/ML. Examples include the Joint Artificial Intelligence Center (JAIC) and AFWERX in the US, the Royal Navy's former NELSON programme, the Royal Air Force's NEXUS platform and the French Agence de l'innovation de défense (AID). However, the current life cycle of these structures suggests they perform well in developing initial capability and iterating their innovation solutions vertically at component or service level. However, they are challenged in scaling horizontally across components, services and agencies.

Figure 1: **Software and AI/ML as a share of major DoD capability-development project costs, and average timelines for software releases (2021–22)**



*32.5% of the projects assessed are not shown because they did not use agile or iterative software-development models, or had incomplete software data, or did not publish a timeline for software releases.
Source: IISS 2023, based on data from United States Government Accountability Office, 'Weapon Systems Annual Assessment', 2021 and 2022.

The implication of this trend is that European, and to a lesser extent American, software capability development remains stuck in a decades-old, costly waterfall model. The latter has been optimised for vertical scaling of hardware-defined capabilities, but it remains inappropriate and inefficient for the horizontal scaling of software and algorithms.

3. Software-defined Defence and Sino-American Strategic Competition

Sino-American strategic competition is the defining feature of the contemporary international system. Technological competition in AI/ML sits firmly at the core of this strategic competition, shaping alliance structures and choices in defence and broader geo-economic concerns.

Western competitiveness in software-defined defence vis-à-vis China maintains a lead for the moment, though that margin is rapidly narrowing as China makes progress in the technological development of AI/ML and other digital advanced technologies, supported by its growing science-and-technology and industrial base and by access to huge private and public funding. The following is a comparative analysis of American and Chinese approaches to software-defined defence.

3.1. US

Over the last decade, two prominent phenomena have accelerated the DoD's recognition of the potential of software-based technologies and the need to develop the right mix of legacy hardware systems and advanced general-purpose technologies such as AI software.

The first was the emergence of low-cost, high-performance cloud computing, combined with advances in chip design and processing speed, battery density and supporting materials development, which together facilitated the 'internet of things' revolution. The number of internet-connected devices increased exponentially, and the volume of data produced unleashed new capabilities across every economic sector.

The second was China's evolution into a geostrategic competitor with ambitions to reshape the international order. A key concern included China's pursuit of technological leadership in critical and emerging technologies through comprehensive industrial policies and military–civil fusion, accompanied by a range of other licit and illicit technology-transfer strategies.

Against this backdrop, US national-security officials in the executive branch and lawmakers in Congress are aligning around discrete strategies to modernise the US military and bolster national security and economic competitiveness more broadly through the identification, adoption and integration of critical and emerging technologies. A preponderance of these technologies – including cyber, autonomous systems, networked communications, and augmented and virtual reality – are software-based, while others – such as biotechnology, hypersonics, quantum sciences and microelectronics – will require specific software capabilities such as AI to mature.

In the military context, the DoD is animated not only by incubating and maturing these technologies. As articulated in the 2018 National Defense Strategy, department leaders are aware that ultimate success 'no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting'.[109] To that end, the DoD is developing new operational concepts that are predicated on software, software-defined hardware, and software enhancements to legacy hardware platforms. Perhaps the signature operational concept that focuses the attention of Pentagon leadership is JADC2, which is an architecture that conceives of every existing or future military asset in space, in the air, on land or at sea as a sensor. Once connected, this network of sensors can seamlessly communicate data; enable AI and machine-learning tools to generate inferences to speed up decisions; allow for more precise and efficient actions; and ultimately create a safer and more secure operating environment for US warfighters.

Despite the strategic alignment, however, the department's progress in modernising the joint force to embrace the changing technological environment has been uneven. The best barometer of the department's progress is perhaps its integration of AI software, given that AI, as a general-purpose technology, will drive modernisation across existing and future weapons platforms, greatly enhance intelligence, surveillance and reconnaissance (ISR) capabilities, and vastly economise DoD business processes such as logistics, healthcare and workforce productivity. Regarding AI uptake in business and weapons systems, there have been notable successes in delivering outsized impact. However, owing to long-standing institutional and procedural path dependencies, organisational and cultural hurdles, and a general technological immaturity, the department still has a long way to go in delivering on these strategies at scale.

3.1.1. Strategic alignment

A consistent theme in DoD strategy documents is that emerging technologies are changing the character of warfare. The 2022 National Security Strategy, in prioritising 'integrated deterrence', seeks to achieve a 'seamless combination of military (land, air, maritime, cyber, and space) and non-military (economic, technological, and information) capabilities'. Key to this ambition is the commitment to modernise the joint force in large part by 'investing in a range of advanced technologies including applications in the cyber and space domains, missile defeat capabilities, trusted artificial intelligence, and quantum systems, while deploying new capabilities to the battlefield in a timely manner'.[110]

Flowing from the National Security Strategy, the 2022 National Defense Strategy outlines the importance of digital technologies in supporting integrated deterrence: '[b]ecause Joint Force operations increasingly rely on data-driven technologies and integration of diverse data sources, the Department will implement institutional reforms that integrate our data, software, and artificial intelligence efforts and speed their delivery to the warfighter'.[111]

This high-level strategy guidance is further realised through three critical defence-technology strategies: the Digital Modernization Strategy, the Software Modernization Strategy and the Data Strategy.

The Digital Modernization Strategy connects the guidance in the National Security Strategy and National Defense Strategy through the lens of cloud, artificial intelligence, C3 and cyber security. Specifically, the strategy highlights that 'cloud and cognitive computing will significantly alter warfighting and defense business operations' and that 'modernization of warfighter support systems will enable improved C2, information sharing, and decision support, through a rich and diverse set of analytic capabilities'. Further, the DoD 'must shape this emerging military-technical competition in AI to our advantage while ensuring a strong commitment to military ethics and AI safety. Decisive warfighting advantage will go to those who integrate and adapt leading-edge technology to create innovative operational concepts with speed and agility.'[112]

The DoD's 2021 Software Modernization Strategy is unambiguous about the role software will play in all domains of conflict, underscoring the need for the department to modernise and reform existing processes to enable decision-advantage through transparent access to critical data and capability. The strategy puts a premium on speed, agile and iterative software development, collection and sharing of data, and utilising open architectures to enable constant capability evolution.

Recognising that datasets for AI training and algorithmic models will increasingly become the DoD's most valuable digital asset, the Data Strategy underscores how important it is for the department to become a data-centric organisation.[113] The strategy highlights that mission commanders, warfighters and decision-makers do not currently have real-time, trusted and secure access to enterprise-wide data. The strategy lays out guiding principles for breaking down data silos, standardising data collection, and encouraging data interoperability and open architectures for development.

Architectural reforms and budgetary support for AI

In a signal to the bureaucracy and to relevant stakeholders in the technology community of its commitment to harness AI solutions for the Joint Force, the DoD has consolidated efforts such as the Joint AI Center (JAIC), the Defense Digital Service (DDS) and the Chief Data Officer in a newly created Chief Digital and Artificial Intelligence Office (CDAO). The role of the CDAO is to:

> lead and oversee DoD's strategy development and policy formulation for data, analytics, and AI; work to break down barriers to data and AI adoption within appropriate DoD institutional processes; and create enabling digital infrastructure and services that support Components' development and deployment of data, analytics, AI, and

digital-enabled solutions. Moreover, CDAO will selectively scale proven digital and AI-enabled solutions for enterprise and joint-use cases as well as surge digital services for rapid response to crises and emergent challenges.[114]

3.1.2. Investment support

With respect to AI, the department has made considerable investments across the military services and the Office of the Secretary of Defense (OSD) components. Relevant investments in AI at the level of research, development, testing and evaluation (RDT&E) and procurement include:

- From FY2016 to FY2025, the department plans to spend USD14bn on AI.[115]
- The Department of the Army requested USD480.2m for AI in its FY21–FY25 budget, up from USD153m in FY16–FY20.[116]
- In the Department of the Air Force, the AI spend in 2019 rose to USD182m, up from USD119m in 2018.[117]
- The DoD launched a USD200m Artificial Intelligence and Development Fund aimed at improving tactical AI at combatant commands by better understanding combatant command data and updating their network infrastructure to improve warfighting capabilities.[118]

3.1.3. Delivering capabilities

These investments and organisational manoeuvres are delivering novel AI capabilities to many parts of the military. Through service R&D labs, innovation entities such as the Defense Innovation Unit, the air force's AFWERX and NavalX, and longer-range technology-focused entities such as the Defense Advanced Research Projects Agency (DARPA), the DoD currently has more than 685 AI projects, including some associated with major weapons systems like the MQ-9 UAV and the joint light tactical vehicle.[119] Additionally, projects include using AI and machine learning to counter adversarial UAS; enable persistent remote sensing for peacetime indications and warning; and enable autonomous teaming. Some notable case studies are highlighted below.

- ***Counter-UAS:*** The DoD leverages autonomous, data-fused and AI/ML-enabled sensor technology to detect, identify, track and defeat adversarial UAS. The counter-UAS technology is deployed at DoD infrastructure, including bases, around the world to protect against adversarial drone attacks.
- ***Synthetic aperture radars (SAR):*** The DoD is utilising satellite-imagery providers that provide faster, more capable and higher-quality satellite images, day or night, in all-weather conditions. The SAR offering includes machine-learning models to augment DoD and US government systems to identify relevant objects in troves of images.
- ***Target recognition:*** The army is actively developing a target-recognition AI capability to support airborne combat operations. The army is also developing a similar capability to sense and identify targets using space-based capabilities such as satellite imagery.
- ***Autonomous teaming of AI systems:*** DARPA is cultivating new approaches for the autonomous teaming of various AI systems – such as AI-enabled drones, robots or satellites – that can react to new or unexpected situations without access to centralised communication and human control. This is particularly important in contested or degraded communications environments.[120]

3.1.4. Impediments to AI integration at scale

There are a variety of reasons for the uneven progress in implementing AI within the department and scaling solutions across the joint force. For this analysis, the focus will be on a handful of separate but related issues that have been the most significant obstacles.

Organisational complexity

Firstly, and perhaps most crucially, there is the immensely complicated structure of the DoD. It is one of the world's largest employers, with 2.8m active-duty, reservist and civilian personnel. It has over USD3 trillion in assets under management and conducts major activities such as acquisitions, command and control, global logistics, health and medical care, intelligence, space operations, facilities management and more. The DoD operates roughly 10,000 operational systems, thousands of data centres, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands of commercial mobile devices.[121] Within this structure, the reality is that the Pentagon is a collection of sovereign entities in the form of the military services, non-combat agencies and combatant commands that are in constant competition for resources and are not necessarily predisposed to overt collaboration.

Further, the Pentagon is subject to the oversight of Congress; lawmakers exert tremendous influence over strategy by granting authority or approving or denying thousands of line items in budgets. In the post-Cold War era, it can be argued that legislators are motivated as much (or more) by political-economic concerns as by geostrategic ones.

Procedural path dependencies

These structural factors are exacerbated by industrial-age requirements, budgeting and acquisition processes that govern the military's ability to invest in, prototype and procure technology. Established by Secretary McNamara in the 1960s, what is now the Planning, Programming, Budgeting and Execution (PPBE) process was appropriate for an era when the DoD was the exclusive investor in and purchaser of technology (such as microelectronics) and the desired products were exquisite, hardware-dominant weapons platforms such as aircraft carriers or tanks, whose production cycles were more linear and predictable.

Software, however, is never finished and its development is non-linear. It is constantly undergoing upgrades to improve functionality and to patch vulnerabilities. Until very recently, the DoD would shoehorn software acquisition into hardware-acquisition pathways, leading to significant delays, cost overruns, glaring cyber vulnerabilities due to lack of upkeep, and a rapid obsolescence as final products were not keeping pace with industry standards.

Mismatched incentives

Flowing from the impediments listed above, incentive structures for stakeholders often work at cross purposes to the goal of ensuring that the US military is AI-ready, leaving the US less prepared to defend itself in the AI era.[122]

- ***Rice bowls.*** Each military service retains high degrees of autonomy over research, development and acquisition processes. As such, service leaders tend to guard programmes, resources and responsibilities to strengthen their position in the competition for resources and to preserve operational ownership in each area. In the context of pursuing joint concepts of operation, as envisioned in JADC2, the reluctance to expose data or allow for API access or common-standards development prevents the seamless integration of sensors in different domains. As a result, each service has a derivative initiative – the air force is actively developing an Advanced Battle Management System, the navy has *Project Overmatch*, and the army is implementing *Project Convergence* – and all are progressing at different speeds and building with heterogeneous technology stacks.
- ***Have vs. need.*** Over the past half-century, the military, Congress and industry have evolved to resist change and procure more of 'what the military has' instead of developing 'what the military needs' for the next conflict. Current incentives, through the defence-budgeting process in particular, commit trillions of dollars to tanks, ships, planes and nuclear weapons at the expense of fielding alternative concepts and capabilities, investing at the right level in new domains such as AI, space and cyber, or investing to support the industrial base in new technologies such as small drones or commercial satellites.
- ***Prime economics.*** The incentives created in the DoD cascade through the defence-industrial base. Specifically, the prime contractors understand the economic advantages of maintaining the status quo. In a world where modular open-source architectures and easily available source code and data are the norm in the commercial sector, the primes are motivated to deliver vertical solutions where they own the intellectual property of the entire technology stack and are not inclined to build open architectures. This contributes to the ineffectiveness of many DoD software programmes. According to Eric Schmidt, the chairman of the National Security Commission on Artificial Intelligence, 'costs spiral due to the need for legacy-system support, while the software is rife with cyber vulnerabilities. When software fails, the cost to fix it can run in the tens or

hundreds of millions, and even then it may ship with reduced capability.'[123]

3.1.5. AI focus going forward

As articulated by the Chief Digital and AI Officer, the DoD recognises that certain practices, such as vendor delivery of vertical AI solutions, will continue. While not ideal, it is the only way that AI can currently be delivered. Moving forward, the CDAO will focus on aligning efforts across the military services on several discrete issues to improve the provision of AI. These include:

- ***Data readiness.*** The DoD has exabytes of data and potentially more. Today, only a fraction of the data is ready to develop and train AI. The CDAO has articulated a vision where, in the hierarchy of needs, DoD must first get the data layer right. To that end, the CDAO will work to find the 15% of the data tables that drive 60–70% of the enterprise value, and aim to centralise those. If the DoD can get those correct, it can allow AI developers and application developers to write back into the DoD's data lake.[124]
- ***Models as a service.*** The DoD currently has very few technologists trained in building models. The DoD should facilitate this training and leverage it in order to keep pace with the commercial sector.
- ***Testing and evaluation as a service.*** Importantly, the DoD lacks a robust process for evaluating AI performance as well as the tools to course-correct. To that end, the Department has drafted a test-and-evaluation framework specific to AI which is intended to provide a sequential process for verifying and validating an AI capability, in line with the DoD's ethical principles and focusing on ensuring security, resilience and robustness. Moreover, this should provide independent and unbiased assessment of the quality and readiness of AI-enabled systems to increase confidence by end users.
- ***AI by design.*** Currently, the DoD utilises AI models that communicate various inferences, and users treat that output as truth. However, underlying these outputs are varying levels of confidence that could introduce grounds for less confident interpretations. The certainties and uncertainties underlying these models are not communicated to the end user. In a military context, treating something as truth can have more serious consequences than in the commercial sector, so the DoD will work with vendors to improve the design of models so that the context around inferences is communicated to the end users.
- ***Cultural and organisational.*** Building AI that is both responsible and functional requires not only algorithmic and infrastructure development but also organisational change. The DoD was not built as a computationally enabled technology company. It is similar to a non-tech company from the Fortune 500 (e.g., a bank) that has core competencies in other areas and needs to leverage AI to accomplish its goals. The DoD has a heterogeneous set of computational systems built over decades, most of its staff are not AI experts, and it was not built with data as a first-class citizen. This means that, in addition to updating computational hardware and software systems to rapidly create, update and continuously deploy models at the speed required, the DoD needs to consider how best to build an AI-driven organisation that does not force AI into existing manual workflows, but rather co-optimises human and machine inputs to best accomplish a given set of end tasks.

3.2. China

Under President Xi Jinping's rule, China has aimed to become a leader in emerging and disruptive technology as part of a wider effort to transform itself from a manufacturing hub to a technological powerhouse. This effort has both military and civilian dimensions, whereby the Chinese Communist Party (CCP) views AI and ML as central to driving economic growth and national competitiveness, as well as key to military transformation and building combat capability for a modern PLA by 2035 and a world-class military by 2049. Militarily, the Chinese government has directed the PLA to become an informatised (信息化) and intelligentised (智能化) military between 2020 and 2049, which will require increasing the integration of digital and information-based technologies as well as intelligent technologies into the military's organisation and capabilities. To this end, the Chinese government has published national-level strategies as well as supported national investment in both the public and private sectors. Through a national-level strategy of MCF (军民融合), the government has also promoted the building of linkages between the civilian and military industries that aims to go beyond the attempts of civil–military integration (军民结合) to create synergies to such an extent that both industries jointly drive forward national economic and military development. However, despite these efforts, China's approach is not without difficulty and obstacles to success, and while the PLA and its affiliated research institutes have become more interested in researching and developing AI/ML for military use, integration of these technologies remains limited.

3.2.1. National AI/ML strategies and relevance for warfighting

The Chinese government has published 11 guiding documents and white papers related to AI/ML. These include the 2015 'Made in China 2025' strategy, and the 2021 '14th Five Year Plan for National Economic and Social Development of the People's Republic of China and Outline of the Vision for 2035'.[125] The National New Generation AI Plan (新一代人工智能发展规划), published in 2017, is most relevant to the development of AI for defence. The plan established initiatives and goals for R&D, industrialisation, talent development, education, standards-setting, and regulation of ethical norms and security.[126] According to the plan, China's AI industry should have been 'in-line' with competitors by 2020, and should reach world-leading status in some AI fields by 2025 and become a primary centre for AI innovation by 2030.

The plan emphasises the importance of MCF to the development of military and civilian AI, and therefore promotes collaboration between the two sectors at foundational levels, such as in data- and platform-sharing. For example, the document states that public-data repositories, standard-test datasets, service platforms and other sources of information should be provided for AI platform-testing and evaluation – including between military and civilian actors. Following that, the plan promotes the joint development of basic theory and key common-technology R&D, and the establishment of normalised communication and coordination mechanisms for scientific-research institutes, universities, enterprises and military-industrial units. In terms of application, the plan emphasises a focus on AI technology for 'command decision-making, military deductions, and national defense equipment'.

Since 2017, national defence white papers and Party Congress work reports have continued to emphasise the importance of emerging and disruptive technologies for PLA joint capability development.[127] Firstly, the 20th Party Congress work report states that the PLA will 'study and gain a good grasp of the characteristics of informatised and intelligent warfare and the laws that govern it, provide new military strategic guidance, and develop strategies and tactics for a people's war'. Secondly, the document puts forward specific areas for improvement. Thirdly, it mandates that the PLA will 'increase the proportion of new-domain forces with new combat capabilities, speed up the development of uninhabited, intelligent combat capabilities, and promote coordinated development and application of the network information system'. Fourthly, the report states that 'high-tech training' will be used to intensify efforts to train the PLA. Lastly, the PLA currently aims to be able to disrupt an opponent's use of AI/ML and big data, in what one AMS researcher calls 'data warfare'.[128] With regard to MCF, the 20th Party Congress work report states that the government will 'better coordinate strategies and plans, align policies and systems, and share resources and production factors between the military and civilian sector'.[129]

However, challenges were also identified in the 2017 National AI Plan, which implied that China, while having advantages, was starting from a low and incoherent base. The document stated that 'we must be soberly aware that there is still a gap between the overall development level of AI in China and developed countries'. In particular, the challenges identified were a lack of original achievements in basic theory, core algorithms and key equipment, high-end chips, major products and systems, and basic materials. The document also stated that the country lacked a comprehensive ecosystem and industrial chain of components, software and interfaces, scientific-research institutions and enterprises, R&D talent, infrastructure, policies and regulations, and standards systems.

3.2.2. National AI effort

According to the 2017 National AI Plan, the Chinese government wanted to cultivate an AI industry worth CNY1trn (USD148.6bn) with related industries worth CNY10trn (USD1.48trn) by 2030. In Beijing, the government has built an AI research technology park worth USD2.1bn together with Chinese technology champions.[130] Specific estimates of how much China spends on AI-enabled technology for military purposes are not available. Some estimates have been made for China's total AI R&D spending. Initial estimates by Ashwin Acharya and Zachary Arnold suggest with low to moderate confidence that China's public investment in AI R&D was in the order of a few billion dollars in 2018 and is significantly lower than previously thought.[131] Additionally, the same researchers hypothesised that the total value of a breakdown of AI R&D spending in 48 plausibly AI-related Chinese government guidance funds may have been between USD2bn and USD8bn in 2018.

As a result of a national and top-down effort, the Chinese government was able to address some of the previously mentioned challenges by 2022, both in R&D, application and integration, and governance of AI within the miliary domain. Detailed information about the central government's resourcing, subsidisation, and efforts to research and develop as well as integrate AI and ML into the PLA is mostly unavailable in open-source literature. However, some reporting does exist that provides inferences into where the PLA might currently stand in its achievements.

For example, cross-sectoral and national-level initiatives continue, such as the annual Data Forum, which is sponsored by the Academy of Military Science and attended by 500 leaders from the Central Military Commission, theatre commands, services and arms, the Academy of Military Science, the National Defense University, and the National University of Defence Technology. The theme of the 2019 conference was 'military big data to promote the development of military intelligence.[132] Published reflections on the conference highlight areas of discussion, from the importance of big data, to building network infrastructure within the PLA to achieve informatisation and share data and intelligence across the military, to the strategic importance of big data and AI/ML for future warfighting.

The PLA continues to gather and develop methodologies for the use of big data (大数据), to the United States' concern. For example, the FBI determined that the PLA was linked to the hack of Equifax in 2017.[133] Experimentation at lower levels of the military has also been reported. In 2021, the commander of the Hebei Armed Police Corps and member of the National People's Congress Rong Jiuhua discussed in an interview with the PLA Daily his own experimentation with big data.[134] For example, he reportedly led an R&D team to explore new ways of building and improving the command system of the Hebei Armed Police Corps using image maps. Rong also expounded the value of integrating big data and blockchain technology to help promote 'the intelligent development of the PLA and continuously improve the joint combat capability based on the information network system'.[135]

At Airshow China 2022 in Zhuhai, uninhabited platforms and systems were on full display. Aviation Industry Corporation of China (AVIC) displayed the Wing Loong 10 (WL-10) UAV in colour, suggesting that the UAV has already entered into service. Chengdu Aircraft Industry Group (CAIG) unveiled a possible mock-up of the new Wing Loong 3 (WL-3) armed drone. China Aerospace Science and Technology Corporation (CASC) displayed a mock-up of the FH-97A UAV, with a computer-generated presentation that showed it operating in an air-to-air networked role with manned J-20A stealth fighters. China Aerospace Science and Industry Corporation (CASIC) displayed an example of the *Tian Ying* (Sky Hawk) fixed-wing drone, which could fulfil a UCAV/ISR (uninhabited combat aerial vehicle/intelligence, surveillance and reconnaissance) role and possibly be deployed on aircraft carriers. However, it is uncertain whether all these autonomous and uninhabited technologies are also described as 'intelligentised'. Land-based uninhabited technology was also on display, and older reports suggest the PLA ground forces have converted older capabilities into uninhabited varieties with some level of suggested intelligentisation. The PLA Navy has also been testing uninhabited intelligent underwater capabilities.[136] A paper published by the chief designer of China's J-20A fighter aircraft, Yang Wei, also stated that China will leverage AI to help pilots process information at each step of the OODA loop in air combat. Chinese researchers have also experimented with the use of AI in cyberspace security and combat.[137] While the PLA's capability development is likely to be more advanced than suggested in open-source information, it is unlikely that the PLA currently fields fully intelligentised capabilities, which PLA and government reporting, such as that in the 20th Party Congress work report, suggests is still aspirational.

In addition to platforms and systems, the PLA has reportedly also been using AI to train pilots. According to one report, the PLA Air Force has deployed AI as simulated opponents in pilot combat training. The PLA Central Theatre Command Air Force held a training simulation in mid-2020 during which top pilots faced AI in exercises. The report states that 'the AI technology-based autonomic aerial combat simulator was jointly developed by the brigade and research institutes'.[138] The report also states that data from exercises is looped back into the AI simulator for further machine learning.

In terms of governance of the use of AI in the military domain, in 2021 the government published China's first 'Position Paper on Regulating Military Applications of Artificial Intelligence', setting forth its position on AI security governance.[139]

It is important to note that in all cases, R&D and the application of AI/ML in the military domain remain a work in progress. For example, a researcher at AMS on big data, Lu Bin, has stated that military big data is still poor in quality, low in value density and incomplete or false. While AI/ML requires sample data, the PLA has very little data on current wars and, logically, no data on future wars. Furthermore, informationisation, which is required for enhanced use of big data and application of AI/ML throughout the military, has still not been completed.

3.2.3. Further challenges

Previous research has already identified that the PLA's development and integration of AI/ML will face several challenges. Firstly, according to Tai Ming Cheung, the PLA's defence acquisition and innovation systems include the monopoly structure of the Chinese defence industry, bureaucratic fragmentation and weak acquisition mechanisms. These structural weaknesses can also be hurdles to military–civil fusion and to achieving synergy between the private civilian and defence sectors.[140] Secondly, Andrea and Mauro Gilli indicate that the limitations of imitation, reverse engineering and cyber espionage mean that China's ability to leverage foreign innovation in areas where it might be lagging behind does not always easily extend to the PLA and China's domestic defence industry.[141] Lastly, as Elsa B. Kania points out, China's need to import the advanced AI chips necessary for AI/ML enablement and deployment is a particular weakness.[142]

The United States' export controls on semiconductor chips to China have complicated this picture even further. The most recent of these controls, announced on 7 October 2022, aims to permanently freeze the Chinese military and civilian high-tech industries where they currently stand, and to further increase the gap between the US and its allies and China in terms of advanced technological capabilities. The measure prohibits US companies from exporting technology, software and equipment to China that is used to produce advanced computing chips and supercomputers, and prohibits US citizens from supporting certain China-based chip companies without a licence from the US government.[143] The new rules also have an extra-territorial element, as they will impact other chip-making producers such as ASML Holding N.V. in the Netherlands. The ultimate impact of these regulations will be determined by the ability of the US and other countries to enforce compliance.

China remains a net semiconductor importer, particularly in advanced chips. In 2021, China imported semiconductors worth USD432bn, and in 2019 Beijing imported 84.3% of the mature-generation semiconductors it used.[144] President Xi has made self-sufficiency in semiconductors one of his main priorities. The state-backed China Integrated Circuit Industry Investment Fund is the largest of such funds in China, with CNY343bn (USD50.6bn) set aside for advancing the country's chip industry. The local governments of Beijing and Shanghai also have their own semiconductor-industry funds worth CNY32bn (USD4.72bn) and CNY50bn (USD7.38bn) respectively.[145] Furthermore, in 2022 some foreign companies attempted to develop semiconductor lines of production solely for the Chinese market, thereby escaping export controls set by the US government.

However, Chinese domestically manufactured semiconductors are not equal in processing capacity to those procured internationally, and developing indigenous advanced semiconductors remains a difficult challenge.[146] China's own microprocessor industry manufactures significant quantities of chips from 24nm and up, but experts argue that Beijing is still a way from being capable of producing microprocessors at the most advanced production nodes.[147] Furthermore, China's national semiconductor fund has been undermined by anti-corruption investigations.[148] Without the ability to produce advanced semiconductors domestically, China's capacity to resolve existing bottlenecks and progress further towards building an informationised and intelligentised military will only become less realistic.

4. European Approaches to Software-defined Defence

As discussed in the previous section, the US and China have a mixed track record of partial successes and partial failures in embracing software-defined defence. But what does this entail for Europe? What perils could be associated with European powers' own efforts to develop software-defined defence as Sino-American strategic competition intensifies? This section will analyse the British, French and German efforts to implement software-defined defence and assess the challenges that stem from Europe lagging behind the two global superpowers.

European approaches to software-defined defence are more modest in scope and ambition when compared to those of China and the US discussed in the previous section. France, Germany and the UK prioritise national AI/ML development in a variety of sensitive domains, including electronic warfare, ISR and strategic C2, as well as in capabilities related to the French and British nuclear deterrents.[149] European countries are often happy to be fast followers of defence-technological progress in the US, and defence software has been a traditional area of weakness of some European states.

French, British and German efforts focus predominantly on accelerating the digitalisation of defence capabilities and put data squarely at the centre. In addition, France and the UK are pursuing the deployment of AI/ML algorithms in defence, underpinned by solid trust and responsible vetting procedures. In Europe, only France and the UK have developed and published defence AI strategies and matured an expansive ecosystem to enable defence innovation, technology maturation, venture-capital funding opportunities and more in support of their efforts. Both France and the UK underline the importance of multi-domain operations underpinned by human–machine teaming and collaborative combat between inhabited and uninhabited capabilities. However, only France is actively implementing large-scale projects to this effect, including *SCORPION* and *VULCAIN*, through which Paris seeks to increase the number of autonomous land vehicles, and the FCAS programme. Large-scale projects are progressing more slowly in the UK.[150] Notable examples include the the *Tempest* fighter jet, the Royal Air Force's PYRAMID project, which seeks to establish a reusable and open-systems architecture and reusable software components for legacy and future air platforms, in order to reduce software-development costs; the Royal Navy's new Naval Strike Network, which incorporates inhabited and uninhabited vessels in battle networks commanded by the Maritime Autonomous Platform Exploitation (MAPLE) platform; and the British Army's Human Machine Teaming project, which aims to develop and deploy a human–machine team brigade by 2025. In contrast, the German armed forces remain among the least digitalised in Europe, which translates into a different and more modest set of priorities in relation to defence software.

The three European countries' efforts towards software-defined defence share an emphasis on data and a long-term perspective on greater integration of modern defence software and AI/ML in defence, which is linked to next-generation capability programmes like the FCAS, the *Tempest* fighter aircraft and the Main Ground Combat System (MGCS). This long-term perspective, mainly as a result of budgetary limitations, frustrates opportunities to upgrade legacy systems in the three countries' inventories using modern defence software and AI/ML technologies. Because their military capabilities, systems and networks are less digitalised and more fragmented than American ones, the challenge for European approaches to software-defined defence is that they require a comparatively higher upfront investment in developing defence-as-a-platform and adopting a software-as-a-service approach, even as they continue to struggle with insufficient technical talent to advance in-house defence-software development.

However, Europeans also diverge significantly in their approach to – and concerns around – software-defined defence because of differences in their defence m is consolidated as the almost exclusive basis for sovereign advanced capabilities for the French military. Resulting capabilities still encounter important interoperability and communications challenges because of proprietary industrial requirements driven by financial incentives. However, the close relationship between the French defence establishment and its national industrial and technological base also provides Paris with potential solutions to alleviate this challenge, and to a larger extent than London and Berlin, who struggle to influence international arms producers.

4.1. UK

Within the UK defence establishment, there is a firm belief that future battlefield advantages will no longer be determined by superior hardware capabilities but rather by a combination of people, hardware and software: personnel and hardware will remain instrumental to warfighting, but software will allow for secure processing, analysis and exploitation of data at the speed of relevance.[151] Software and data are expected to enable decision-advantage for British troops and decision-makers. The combination of deployed military software and hardware is expected to regenerate lost mass and manoeuvrability for the British armed forces.[152] And algorithms may even offer asymmetric advantage on the battlefield in the event of defending against Russia and China as part of multi-domain integration.[153]

4.1.1. Data as the source of asymmetric advantage

The UK's approach to software-defined defence puts data at the centre of efforts to adopt and integrate software and emerging technologies in defence applications to achieve an asymmetric advantage against strategic adversaries like Russia and China. Given the emphasis on data as a core resource in future warfare, the Ministry of Defence has adopted a whole-of-defence, system-of-systems approach to reorganising and restructuring approaches to capability and software development, and views disruptive and emerging technologies as central to force structure, procurement strategies and its overall approach to future conflict.

4.1.2. Policy alignment

There is alignment across different defence stakeholders around a strong sense of British prioritisation of data in defence, which is underpinned by key strategic and policy documents. The 2021 'Integrated Review of Security, Defence, Development and Foreign Policy' emphasises the importance of sustaining strategic advantage through science and technology. The 'Integrated Operating Concept', first published in 2020 and updated in 2021, highlights that 'technologies such as pervasive availability of data via enhanced cloud connectivity, machine learning and artificial intelligence, and quantum computing will allow not just a new generation of weapons systems but an entirely new way of warfare'.[154] This has translated into an increased investment in cyber and digital capabilities in the ministry's 'Defence Equipment Plan' for 2022–32.

Furthermore, the UK's Data Strategy for Defence emphasises that by maximising value from data via an integrated digital environment across defence, decision-makers can take decisions faster by using software to derive insights from data, resulting in warfighters gaining real-time access to information and, in turn, operational and decision-making advantage.[155] And the Digital Strategy for Defence released in April 2021 underlines the importance of data-driven systems 'where "software defined capability" gives (…) an asymmetric edge by sensing, recognising and responding to new opportunities and threats' faster than adversaries.[156] Under the Digital Strategy for Defence, the UK aims to achieve three strategic outcomes by 2025: a 'Digital Backbone' enabling the flexible, seamless and secure real-time sharing of data across the enterprise; a 'Digital Foundry' that is the ministry's software and data analytics factory; and a skilled community of digital specialists who can support the ministry's digital transformation.

In 2022, the UK released its Defence Artificial Intelligence Strategy, becoming the second European country to publish such a programmatic document. The document adopts a '"systems" perspective' for AI procurement that focuses on 'outcomes, delivered through clear frameworks and processes, and guided by [the] conviction that AI can be a powerful force for good'.[157] The document proposes a pathway to enhance existing safety and regulation practices, in compliance with democratic principles and international law, and sets a clear framework to ensure UK adoption and use of AI in defence is trustworthy and responsible.[158]

However, human factors and digital enablers of AI/ML such as data, software and digital infrastructure remain important challenges. The strategy does not identify or prioritise a set of software-defined capabilities, though it does underline that the UK is seeking to deploy AI/ML to achieve strategic and operational advantage against adversaries.[159] The document underlines a high level of ambition, based on an awareness of the fact that London is not competing at the level of either Washington or Beijing: 'Our vision is that, in terms of AI, we will be the world's most effective, efficient, trusted and influential Defence organisation for our size.'[160] In an effort to manage expectations, the strategy underlines that in the short and medium term the UK expects to deploy mainly enterprise-and-support AI rather than operational battlefield algorithms. Further clarity is expected from the Implementation Plan of the Defence Artificial Intelligence Strategy and from potential 'AI readiness' guides for individual units on the development and adoption of AI/ML to de-risk the technologies at a more granular organisational level.

4.1.3. Software-defined capability priorities

The focus in UK capability development remains on how data can enable new digital technologies to be exploited and scaled in the armed forces, rather than on the actual process of shifting from a hardware-oriented to a data-based and software-defined defence approach. The Digital Backbone and Digital Foundry have become the focal points of the ministry's efforts. Defence Digital's slow progress towards building a capability that incorporates a common standards-based, interoperable system throughout the ministry has often frustrated other software-defined defence initiatives within the military services. This common standardised foundation developed by Defence Digital would be expected to allow Defence to exploit curated data as a strategic asset and to enable a strategic shift to software-intensive capabilities. The UK's challenges in building a mature and reliable digital backbone for its armed forces are not unique, as the US DoD's ongoing struggle to establish a Joint Common Foundation has proved.

Despite tangible progress in the implementation of the Digital Backbone and Digital Foundry, in line with agile models of capability development, there is also widespread recognition that technology teams across the defence establishment have not yet fully adopted new standards and practices. Defence Digital's programme- and project-delivery track record continues to be affected by 'a lack of skilled and experienced personnel, immature project controls, and a culture focused on the approvals process rather than outcomes', which undermines its ability to affect change across the defence sector in the 90 programmes it currently coordinates.[161]

The sense of muddled UK capability priorities is reinforced by recent announcements about cancellations of future capabilities such as the *Mosquito* uninhabited loyal-wingman programme, which seemed to be at the core of regenerating mass for the Royal Air Force and enabling collaborative combat alongside inhabited and uninhabited versions of the *Tempest* fighter aircraft and uninhabited *Alvina* drones.[162] Another relevant example is the unexpected reform of the Royal Navy's NELSON programme, an internationally appreciated brand for the service which was increasingly successful in regular and frequent software releases.

More recently, UK Strategic Command announced a focus on three priorities in software-defined capability development in the coming years: cyber, the electromagnetic spectrum and enhanced situational awareness. However, there is little detail about how software-defined defence will shape the UK Strategic Command's capability priorities without the capability provided by the Digital Backbone, which has been slower to achieve than initially planned. In January 2023, the Ministry of Defence published 'Joint Doctrine Note 1/23', which provides a blueprint of changes in methodology, practices and capabilities underlying ISR to accommodate both more data-varied and data-intensive practices as well as to facilitate end-to-end electronic workflows in ISR.[163] However, more work is needed to flesh out mature doctrine and operational concepts that build on and fully exploit a software-defined defence approach enabled by data, software and AI/ML.

4.1.4. Software-defined defence and capability development

Software-defined capabilities are included as part of efforts in adopting emerging technologies in defence, and there are efforts across the defence sector and the services towards incorporating agile and iterative software capability-development models into R&D and capability-development pathways. The UK Strategic Command's jHub is developing and testing a 'Sustainable Tech Adoption Model' (STAM) that is exploring new ways of working with industry to procure new capabilities.[164] Next-generation flagship capability-development programmes like *Tempest* are implementing a 'digital-first' approach to digitally engineer, build and test the concept. And the UK already deploys several defensive systems enabled by rudimentary automation, data-management-as-service and AI-powered analytics.[165]

In 2022, Defence Digital signed a three-year GBP75m (USD90.3m) contract with Palantir which will help it 'exploit data at scale and speed to make faster, better decisions' by unlocking data from legacy operational systems, fusing operational and sensor data for decision-making support, enabling mesh networking among different operational systems and sharing data across the enterprise.[166] Similarly, in 2021, the Ministry of Defence awarded a three-year contract to Anduril to support the implementation of the *TALOS* programme, which seeks to trial an AI-enabled advanced base protection system.[167]

The army is implementing several simultaneous testing and experimentation projects, including the Human Machine Teaming project, which focuses on the integration of robotics and autonomous systems (RAS), *Project WAVELL*, and *Project Mercury*. Together, the projects seek to incorporate agile software and capability-development pathways to accelerate innovation uptake in the armed forces, deliver a brigade-level component enhanced with robotic systems and an integrated sensor-decider-effector chain by 2025, and evolve new tactics and operational concepts to deliver maximum deterrence and fighting power. These projects use shorter iterative cycles of one to two years to experiment with and test new open-architecture-based capabilities and strict government-owned data. The Human Machine Teaming project incorporates software-as-a-service and data-management-as-a-service approaches to deliver human–machine teams on the battlefield, and *Project Mercury* is focused on developing next-generation autonomous land capabilities across the support and combat spectrum. The army's 'Land Intelligence, Surveillance, Target Acquisition and Reconnaissance' programme seeks to deliver an adaptable and robust system based on an open-system architecture built for multi-domain integration and interoperability with allies. The programme's official description suggests it uses an approach based on the disaggregation of sensors, human deciders and effectors, working in an end-to-end electronic workflow environment where command is centralised and tasking decentralised.

Similarly, the Royal Navy's approach to the implementation of the Digital Strategy for Defence highlights several principles consistent with a software-defined defence approach, including a systems-of-systems approach of disaggregating sensors, human deciders and effectors that is enabled by an end-to-end AI-enhanced architecture, has a cloud-first focus across the strategic, operational and tactical levels, and is autonomous by default implementation. These principles are embodied by the navy's platform *Pyramid.* For example, the *NavyX* Accelerator seeks to transform the adoption and integration of cutting-edge technologies in defence through an extensive testing and experimentation ecosystem. Since scrapping the NELSON programme in 2021, the navy has transitioned to building a Software House under the 'Data and Navy Applications' initiative. Launched in 2022, the initiative seeks to deliver new reusable capabilities based on a common standard; build a common data fabric for the navy; and enable an end-to-end electronic workflow between existing legacy capabilities to ensure more utility and functionality is derived from existing inventories. Supported by the navy's Defence Transformation Fund, the navy is experimenting with intelligent-ship designs that build on electronic workflows between sensors, human deciders and effectors, autonomous mine countermeasure systems, and littoral strike ships. *NavyX* is deploying a new testbed ship, the *XV Patrick Blackett*, for testing and experimentation of new digital and software ship environments.[168] Royal Navy sources are optimistic the ship may soon become its first digital-experimentation facility for autonomous capabilities.[169] The Royal Marines' 'Autonomous Advance Force' initiative has repeatedly experimented with a variety of surface, air and land tactical uninhabited vehicles.[170]

In addition, in 2022, Defence Digital deployed the Defence DevSecOps Service (D2S) 'to accelerate the delivery of common platforms and services to enable data, digital and AI exploration', and the Ministry of Defence updated its R&D framework to restructure grants around shorter project development and monitoring phases.[171, 172] After the COVID-19 pandemic, UK innovation agencies like the Defence Science and Technology Laboratory (Dstl) and Defence and Security Accelerator (DASA) increased the frequency of challenges, competitions and innovation awards, making them bi-monthly.

Furthermore, UK testing and experimentation in capability development and operational-concept development across UK Strategic Command and the services greatly benefit from enhanced cooperation with the US and also with other allies in NATO and the Indo-Pacific. For example, the army's software-defined innovation efforts are significantly enhanced by its participation in the US Army's *Project Convergence*, the Royal Navy's digital-transformation agenda is supported by cooperation in the 'Tech Bridge' initiative with the US Navy and collaboration with its Task 59 in the Gulf, and the Royal Air Force has benefitted from training on the US Air Force's advanced surveillance system, the *GHOST Mk4* UAS.[173, 174, 175]

4.1.5. Further challenges

While these are positive steps in the right direction, more time is needed to assess whether this transition is a significant step away from waterfall capability-development processes towards more agile, iterative and user-driven ones. For each of the positive examples discussed above, there are just as many complex UK capability-development programmes that continue to treat software as an adjunct to military hardware because the UK continues to pursue a capability-based approach. *Ajax* is the latest and most pertinent example.[176] The Ministry of Defence has similar problems with the *Watchkeeper* UAS, not least because of software design and incomplete requirements and specifications.[177]

Furthermore, agile and iterative software- and capability-development practices are integrated mainly in newly launched or unfunded capability programmes, and compressed delivery times for new capability and functionality are yet to be made clear. This creates added risks to projects and agile development practices, as budgetary constraints demand that critical trade-offs are made between introducing new capability programmes and sustaining existing, albeit possibly problematic, ones.[178]

The Ministry of Defence is already using software-as-a-service contracts for advanced analytics or for service-wide data management. However, this approach could be further scaled across the defence establishment. This is all the more important since the Ministry of Defence will continue to struggle with severe shortages of human skills for rapid software and AI/ML development in the medium term. The ministry is working on an AI skills strategy, though its effects could take as long as a decade to materialise.

Further work is needed on the implementation of the Data Strategy for Defence to maximise utility out of defence data. Currently, defence staff are struggling to cope with severe data-storage constraints and a lack of clear understanding of how to assess data to ensure valuable data is not automatically discarded before it is fully exploited.[179]

Furthermore, greater transparency is needed around risk assessments of software and AI components in defence capability-development projects. Clearer delivery timelines for software-defined capabilities, enabled by the application of agile development procedures, are also needed. Closer alignment is also necessary between initial efforts towards agile software and capability development and modernised approaches to testing, verification, validation and certification methodologies to avoid significant challenges in field testing and experimentation across the services.

Finally, the Ministry of Defence is trying to engage more with start-ups and small- and medium-sized enterprises that develop cutting-edge advanced technologies. However, there are important concerns around the sustainability of resilient ecosystems for dual-use and defence-specific technologies. The UK national ecosystem is significantly smaller than the United States' and China's, and even though the UK remains the most attractive tech ecosystem in Europe, it is far from complete and resilient in all its sectors. Space is a very good case in point, but quantum, directed energy and biotechnologies are at risk of following in its footsteps. This has implications for the ministry's continuous ability to draw on its technological-industrial base in critical sovereign-technology areas. It may equally require a reconsideration of current defence R&D practices to make innovation competitions easier and more attractive for a wide range of private-sector actors, as well as to incentivise closer cooperation between traditional and non-traditional private-sector partners in delivering advanced capabilities to the warfighter.

4.2. France

France was the first European nation to publish a defence AI strategy in September 2019 and to prioritise the importance of data and new technologies, notably AI and quantum, for the future of warfare. The link between data and AI was clearly stated in the strategy. The document established a new framework for governance of data within defence and identified the following priority areas for AI use cases: decision support in planning and execution, collaborative combat, cyber defence and influence, logistics, support and operational readiness, intelligence, robotics and autonomy, and administration and health. While specific technologies are not an end in themselves, the French armed forces seek to use AI for 'ensuring that the armed forces' decision-making processes have the necessary operational superiority to give them the upper hand over many types of adversary'.[180] Importantly, the document identifies a pressing need to achieve technological sovereignty in a global technological landscape of new technologies, such as AI, that is dominated by the US and China.

4.2.1. Policy alignment

There is a strong alignment between French policymakers and military leaders regarding the role of emerging technologies in ensuring Paris retains its autonomy over assessment and decision-making in defence matters. The ability to exploit data and advanced digital technologies (e.g., nuclear and space) is widely acknowledged as a prerequisite for French geopolitical relevance, military-technological superiority and defence-industrial competitiveness.[181, 182, 183]

The 2022 'National Strategic Review' emphasises that in 'an increasingly competitive and complex international context, France must focus its efforts on raising its level of knowledge, its appreciation of competitors and adversaries, and anticipating their intentions' through 'continued investment in technological capabilities to exploit the ever-expanding volume of data, in order to share relevant information with decision-makers and action-takers in a timely manner'.[184] Furthermore, the document highlights that 'technological equalisation helps to make numbers important again', and that by sometimes taking a more agile approach and by sheer weight of numbers, France's 'strategic competitors have the capacity to tip the regional balance, such as Iran in ballistics'.[185]

This alignment in relation to emerging technologies extends to the importance of moving towards strategic autonomy – and defence-technological autonomy – in a European context as well as enhancing the role and contribution of the French armed forces to NATO. Advanced technology solutions, agile procurement and better integration of innovative technologies that ensure interoperability with allies and partners and are developed in a whole-of-government approach are key to restoring European and French superiority in the warfighting domain.[186]

To this effect, in May 2020 the Ministry of the Armed Forces issued an official guideline related to defence innovation, focusing on attracting and integrating new technologies into defence applications. The document organisationally restructured R&D processes within defence and laid new foundations for R&D governance, actions and funding. The annual *Document de Référence de l'Orientation de l'Innovation de Défense*, which features data and AI-driven capabilities among its highest priorities, set goals for both long-term, planned innovation that is needed to prevent technological surprise, and for the short-term, open innovation intended to capture technological advancements in the private sector and adopt them in defence applications.[187, 188]

4.2.2. Organisational adaptation

The French focus on R&D and dual-use technologies originating in the private sector has been accompanied by a series of organisational transformations within the Ministry of the Armed Forces intended to reinforce the R&D sector and provide the French armed forces with access to a sovereign supply of critical technologies for defence. These have included the establishment of the Defence Innovation Steering Committee (Comité de Pilotage de l'Innovation de Défense) and the Innovation Acceleration Standing Committee (Comité Permanent d'Accélération de l'Innovation) to manage and steer defence-innovation priorities and activities across the ministry, as well as the Defence Artificial Intelligence Coordination Cell (Cellule de Coordination de l'Intelligence Artificielle de Défense) to coordinate all defence projects related to the development, adoption and integration of AI in defence.

Furthermore, in September 2018, President Macron established the AID under the Directorate General of Armaments (DGA), the ministry's capability-development and procurement powerhouse. The AID was tasked with coordinating innovation across the defence enterprise and with the civilian sector to better attract and exploit dual-use and general-purpose technologies for defence applications. The AID implements four types of projects focused on driving innovation:

- defence technologies projects: those that refine the technologies necessary for military requirements and are the main vector for planned innovation;
- innovation-acceleration projects: those that capture innovations from the civilian sector, adopt them for military use and further develop them with ministerial support. Innovation-acceleration projects represent the second-largest number of projects under implementation by the AID (134 out of 454 projects);[189]
- participative innovation projects: those originating from French military personnel and focused on specific use-cases at earlier stages;
- research projects: those geared towards long-term research and future strategic technologies, usually in partnership with academia, research organisations, schools or companies. As of 2021, research projects represented the largest share of the projects implemented by the AID (169 out of 454 projects).[190] However, the AID has faced strong criticism for the mismanagement of these projects and for failing to rapidly contract projects developing new technologies for defence applications.[191] Though contracting should take 90 days at most, the AID's timelines extended to well over nine months in 2020 and 2021;
- in addition, the AID coordinates *La Red Team*, which is tasked with developing defence-relevant foresight scenarios of future conflict and strategic competition.

In April 2021, the Ministry of the Armed Forces launched the Digital Defence Agency (l'Agence du Numérique de Défense, AND). The new agency is responsible for managing 'complex or high-stakes digital projects' within the framework of the ministerial policy relating to digital technology defined by the Directorate-General for Digital Affairs (Direction Générale du Numérique, DGNUM).[192]

The newly created structures are focused on enabling the French transition to a system-of-systems approach to defence digitalisation and innovation. The digitalisation of defence in the French context has incorporated elements related to the digitalisation of military equipment, systems and networks, as well as the progressive incorporation of new and advanced technologies like AI in defence applications. Furthermore, the ministry has established an ethical committee to oversee the responsible development and use of key advanced technologies in defence, including AI, quantum, biotechnologies and human enhancement. The overarching logic of this process is in line with foundational tenets of software-defined defence, notably data, software and AI/ML algorithms.

4.2.3. French focus on high-intensity warfare and software-defined defence

The French approach to defence innovation has evolved during the last five years. Importantly, the French armed forces' approach to future conflict has shifted in 2022 towards a prioritisation of high-intensity warfare and away from its previous focus on low-intensity and counter-terrorism warfare. The transition implies a move away from innovation and modernisation of the 'middle segment' – in which the French military is prepared to address conflicts and threats across the low- to high-intensity, state and non-state threat spectrum by maintaining a full-spectrum military capability – towards high-intensity warfare.[193, 194] This is a requirement of the current period of renewed and intensifying great-power competition, in which technological and information superiority within multi-domain operations are the markers of battlefield competitiveness.

High-level military officials have publicly acknowledged that France's focus on the middle segment in the 2000s and 2010s led to a depletion of specific capabilities even as the force remained highly expeditionary. This focus also ossified the long-term planned innovation pillar of French R&D to such a degree that in 2021 over 95% of innovation projects related to emerging technologies like AI and data science were linked to existing programmes of record for next-generation capabilities, such as the FCAS.[195] France's focus on planned and incremental innovation, in which new technologies are adopted as part of next-generation capabilities or mid-life upgrades of legacy platforms, created an environment in which emerging technologies best succeed when tied to existing programmes.[196]

The result was an innovation cycle in which technologies that were not linked to existing programmes risked being underfunded or deprioritised and deemed to have a low technology-readiness level, which could adversely affect the continued R&D of such technologies despite their potential use in future warfighting operations or for future modernisation needs. Paradoxically, technologies linked to high-profile capability projects, like FCAS and *SCORPION*, were often prioritised despite lower maturity levels, leading to deadline and cost overruns. In theory, the ministry restructured administrative processes within platform-driven capability-development programmes, enhanced programme monitoring to ensure incremental integration of technologies in capabilities, and sought greater collaboration with end users to facilitate a genuine system-of-systems approach.[197] However, most efforts towards defence innovation and digitalisation in AID, for example, placed more emphasis on supporting the civilian-industrial base for AI development, among other technologies, than on facilitating their rapid adoption and integration into French military systems.[198]

A reorientation towards high-intensity inter-state conflict carries important implications for the approach to capability development and procurement as well as for France's overall preparedness, as French military officials acknowledged in 2022 (prompted among other reasons by the ongoing war in Ukraine).[199] This transition is still too recent to allow an assessment of its impact on the French embrace of software-defined defence or to determine whether it has changed the ministry's organisational innovation culture, which, as in the case of the UK, is often risk-averse and deprioritises disruptive innovation.[200] However, it is a step in the right direction for the armed forces to align threat assessments and capability priorities, and to seek to accelerate the adoption of new technologies in defence, not just as part of the next-generation capabilities to be deployed in the mid- and late-2030s but also within the broader armed forces.

4.2.4. Software-defined defence and French capability development

The Ministry of the Armed Forces already deploys data science and AI applications for advanced analytics, predictive maintenance and other tasks. For example, France is using software-as-a-service solutions for the exploitation and analysis of data generated by its space-based assets, AI-enabled predictive maintenance and munitions health solutions, sensor-data fusion and analysis for the *Rafale* fleet, as well as predictive big-data analytics and digital-twin solutions for the *Falcon*.[201, 202, 203] In addition, the French armed forces are already deploying and experimenting with a wide range of uninhabited land and aerial vehicles.[204]

Paris has also implemented several flagship projects that leverage data, software and AI/ML in defence capabilities. One of them is *ARTEMIS* managed by the AND, which is building an integrated and sovereign digital backbone for the French armed forces, equipping them with the ability to flexibly fuse and exploit big data, and use a cloud-native architecture and software factories. The project was launched in 2017, with the first year-long phase seeing three concepts proposed by Capgemini, Atos, Thales and Sopra Steria competing against each other. In this phase the requirements included a core execution environment; adequate computing and storage capacity; a software factory and a sandbox for the development and testing of new software and algorithms on real data in a controlled environment; and a software-development kit. And the ministry appeared to adopt an agile development model that emphasised early collaboration with the end users and a modular approach to building and upgrading the capability.

In phase two, launched in 2018, Atos and Thales were chosen to mature and demonstrate their concepts in six different use-cases: processing of heterogenous big data; cyber security; staff-health monitoring; technical and economic intelligence; maintenance; and fleet monitoring.[205] An interim capability version of *ARTEMIS*' technology demonstrator is already in use with the French armed forces and use-cases are subject to several pilots testing the capability. During phase two of the project, market-consolidation dynamics led Atos and Thales to establish a joint-venture company, ATHEA, which became the sole designated contractor for *ARTEMIS* in phases two and three, the latter launching in mid-2022.[206] Capgemini and Sopra Steria became subcontractors to the project. Phase three foresees the industrial roll-out of the technology across the ministry and the military services by 2028.

As the armed forces transitioned towards prioritising high-intensity warfare in 2022, other ongoing projects that focus on the AI-enabled exploitation of big data and autonomous capabilities have gained renewed importance in the French defence ecosystem.[207] Notable examples include *SCORPION*, which is recapitalising the lighter segment of land capabilities in the army with a modernised C2 and communications system; *TITAN*, which is modernising the army's high-intensity-warfare capabilities for high-connectivity, networked, multi-domain combat; and *VULCAIN*, which seeks to expand the number of autonomous land logistics and combat vehicles in the army every few years. In the air domain, the FCAS and 'Man-Machine-Teaming' programmes were developed in coordination to provide a sixth-generation manned and uninhabited air-combat capability for multi-domain operations. The programmes are already developing several AI-enabled capabilities for data fusion as well as analytics for enhanced situational awareness and monitoring of pilot health. Furthermore, in April 2021 the ministry launched the *BRASIDAS* project, which is expected to deliver an AI-enabled predictive maintenance solution for the H225M *Caracal* helicopter and *Patroller* drone fleets.[208] The project is also expected to extend to vertical-lift fleets, such as France's AS532UL *Cougar* and *Tiger* helicopters and the *Rafale* and *Mirage* 2000.[209] Project *SIBIL (Système d'information pour la prévision des besoins et l'innovation logistique)*, which uses algorithms for the predictive maintenance of land vehicles, is under experimentation with the French army. All these projects will be enabled by a combat cloud foundation.

4.2.5. Further challenges

The French Ministry of the Armed Forces has prioritised elements of a software-defined defence approach in their vision of exploiting data, AI/ML and digital solutions in defence. However, several concerns persist. Notably, though budgetary allocations for the development and implementation of digital infrastructure for modernised legacy systems or for new capabilities have increased, reaching EUR2bn (USD2.4bn) in 2023, many key digital-infrastructure projects are delayed in comparison to the capability-development timelines. Examples include digital infrastructure for the *ARTEMIS*, *SCORPION* and *Rafale* upgrade programmes.[210] This could lead to delays in the operational deployment of new functions and capabilities. Moreover, obvious gaps in French digital-infrastructure planning – such as the lack of any ongoing projects to deploy 5G technologies in defence applications – could pose a different type of challenge to the adoption of AI and more advanced software in defence, even as France is the European leader in satellite-based communications and intelligence.

Official sources have presented the flagship capability-development projects discussed above as examples of agile integration of new technologies into defence capabilities, based on modular, open architectures. However, analysis of these programmes suggests they are developed through a classic waterfall capability-development model, where software development is often separated into different strands. While this is the case for the *SCORPION* and FCAS projects, *ARTEMIS* elicits similar concerns. Important questions remain unanswered about the full capabilities and functionalities of *ARTEMIS* in phase three, solutions for substantial data and communications challenges across the enterprise, the overall cost of the contract, and the general approach towards upgrades, maintenance and new functionality integration, which are key to a software-defined defence approach. Therefore, it is unclear whether the Ministry of the Armed Forces is genuinely moving towards more agile, iterative and modular approaches to defence-capability development.

Furthermore, it seems the French defence establishment is being pulled in different directions by different institutional interests. France's 2019 defence AI strategy sought to increase the defence establishment's appetite to develop capabilities based on new technologies by establishing a formal process to monitor whether they are trustworthy and responsibly used by the armed forces. However, the organisational culture within the French defence establishment remains risk-averse and oriented towards long-term incremental innovation and technological uptake. While this is also true of other European countries, in France there is a significant disconnect between the urgency of the policy narrative around the technological and digital modernisation of the armed forces and, in practice, the misalignment of innovation and procurement.

4.3. Germany

In 2018, Germany's then-minister of defence Ursula von der Leyen acknowledged that 'every "battle", whether it is fought on land, at sea or in the air, is at the same time always a battle for "information power", which is why armed forces such as the Bundeswehr need their own networks and software to be both functional and resilient'.[211] She also acknowledged the need to 'develop processes in order to securely and profitably use the exponentially growing amount of information and data we can collect today thanks to modern technology'.[212] This acknowledgement is not unique among the German political and military elite, where there is wide acceptance of the need for the Federal Government and the armed forces to digitalise in order to take advantage of and prepare for emerging and disruptive technologies. While the need for greater digitalisation of the German armed forces has become greater over the last five years, concrete actions have not been forthcoming. As a result, out of the five case-study countries, Germany remains the furthest away from embracing a software-defined defence approach.

4.3.1. Policy alignment towards a society-first approach

The lack of concrete action towards the digitalisation of defence and adoption of advanced technologies like AI/ML in defence stands in harsh contrast to the Federal Government's policy interest and investment in emerging technologies and data exploitation in a civilian, economic and industrial context. Indeed, there is broad political consensus in Germany around increasing the country's technological and data sovereignty. For example, Germany's 2020 Artificial Intelligence Strategy emphasises key societal use-cases in the economy, health and industry, the need for action that consolidates AI skills in society and consolidates national and cross-border European AI ecosystems, and the fostering of an ethical approach towards the development of trustworthy and responsible AI applications.[213]

Furthermore, the country's 2021 Data Strategy underlined the need to improve data provision and secure data access at the infrastructural level, to promote responsible data use and tap potential for innovation, to improve data skills and establish a new data culture in Germany, and to make the Federal Government a world leader of the new data culture. The document highlighted the potential for gaining geo-economic competitiveness by incentivising data-centric innovation, including in new technologies such as quantum computing, while expanding Germany's technological sovereignty and establishing a national regime for data security and protection by design. The Data Strategy announced the government's intention to create a shared data pool that allows for a standardised, accessible data format for use by any federal authority, although standardisation was acknowledged to be a substantial challenge.[214]

By contrast, there is no political consensus around concrete actions towards the digitalisation of defence and the adoption and integration of emergent technologies like AI/ML, despite a high-level policy prioritisation of a data-driven approach. The Ministry of Defence adopted a Defence Data Strategy in 2021, in line with multinational developments in NATO and the EU.[215] The document set the objectives of establishing a defence data-governance framework and a standardised data infrastructure; achieving a data-oriented organisational culture and increased institutional data literacy; enhancing innovative use of data, ensuring data quality and availability across defence; and enhancing the operational resilience and readiness of IT networks and weapons systems while reducing their life-long costs and enabling big-data analytics.[216] Other service-level policy guidance on defence data management, like the Bundeswehr's digitalisation strategy, remains classified. The ministry is reportedly implementing over 1,000 digitalisation projects, based on a phased 'connecting-islands-of-digitalisation' plan, many of which are component- and service-level initiatives facing long delays due to legal and bureaucratic bottlenecks.[217] Explaining the Bundeswehr's incremental approach to digitalisation, the digital officer for land-based operations said this: 'We have to build small, manageable islands, fully digitalise them, bring about success, and then carry that success over into other areas by creating new islands. We are not starting with full divisions or brigades, so not with 30,000 or 10,000 people, but rather with a battle group. That is around 1,500 people and 800 vehicles. And those are going to be fully digitalised in the system.'[218] There is no public evidence of the ministry moving towards enterprise-wide system-of-system approaches consistent with multi-domain operations and a software-defined defence approach.

Moreover, the 2020 updated Strategy Paper of the Federal Government on Strengthening the Security and Defence Industry featured four digital technologies out of the total eight key technologies identified as important for the future of the German armed forces: security-relevant IT and communication technologies, AI, sensors and network-enabled operations/crypto technologies.[219] A research branch of the Bundeswehr emphasised the need to adopt networked military capabilities and achieve mass and manoeuvrability as fundamental measures to prepare for the future of warfare and an increasingly transparent battlespace covered by smart networks of active and passive sensors.[220]

Meanwhile, the German armed forces are struggling with severe connectivity and communications challenges, where legacy systems cannot share data either with each other or with close allies. The prioritisation of the digitalisation of land forces is linked to the TEN and D-LBO projects, which are interdependent and driven by multinational requirements for NATO and EU missions and operations. For example, project TEN is modernising and digitalising tactical communications and data-exchange capabilities between the German and Dutch land forces, whose military equipment was not previously interoperable. In 2019 the Ministry of Defence launched SysZ Digla, the digital organisational and functional element of the digitalisation of land forces, through the D-LBO and TEN projects. All digital projects within the Ministry of Defence are built on reusable standard building blocks to enhance interoperability and diminish life-long costs. However, the focus of the ministry's digitalisation activities remains the digitalisation of the defence enterprise and business systems, with measures to increase the digitalisation capacity of weapons systems 'still in their infancy' according to German official sources.[221] In 2021 the ministry was managing 81 digitalisation activities, with implementation timelines mostly of one to four years, or longer in a few cases.[222]

4.3.2. German software-defined defence innovation

The German armed forces operate several platforms and types of ammunition with some or full autonomous capability. This includes the autonomous functions of aid-defence systems, UAVs such as the *Puma* 3 AE tactical UAV, and the *LUNA* UAV, the *Harop* loitering munition, uninhabited ground vehicles (UGVs) like the THeMIS tactical UGV, and other autonomous counter-mine clearance and underwater autonomous ISR capabilities.[223] In addition, Germany participates in the FCAS project which, as discussed in the previous subsection, incorporates several software-defined elements. However, Germany has opted out of an uninhabited version of FCAS.

In addition, the Ministry of Defence is already using an AI-enabled early-warning system from crisis management as well as AI-enabled military personnel-health and travel applications, with other projects currently under development.[224, 225]

Digitalisation and AI adoption is provisionally part of other ongoing modernisation efforts. One example is the *HERKULES* follow-up project, which enabled a basic cloud infrastructure for the Bundeswehr and the digitalisation of its healthcare databases and services to personnel.[226] Another is the MESBw, which is modernising command, control, communications, computers and intelligence (C4I) software and infrastructure for the armed forces based on an open architecture model that interconnects legacy proprietary systems, such as command and weapon-deployment systems (FüWES) and weapon-system platforms.[227] Since 2018, the special-operations forces have successfully tested the 'Multi-sensor real-time combat in an ad hoc mesh network' (MEGA) prototype, while other units in the Bundeswehr have tested Distributed

Cyber Reconnaissance as a Service (DCR) prototypes.[228] The ministry is also slowly rolling out the Harmonisation of Management Information Systems (HaFIS) project to modernise the mission-planning tools of stationary and deployable command posts. As the ministry is seeking commercially available, off-the-shelf software within the aforementioned projects, the largest risks associated with the projects stem from the lack of supporting infrastructure and digital skills, rather than from low levels of technological maturity as in the cases of France, the UK and the US.[229]

Most ministry and Bundeswehr innovation initiatives or strategies for data-driven, software-defined or AI-enabled capabilities are tied in with Germany's broader goal of securing EU defence initiatives and digital sovereignty, or take a back seat to existing NATO goals, development strategies or modernisation/innovation requirements. Existing efforts include software-defined radios as part of the EU *European Secure Software defined Radio* (ESSOR) project and some development of AI-enabled military systems, such as the FCAS programme with France and Spain.

Little innovation is practised exclusively by Germany for its own benefit.[230] The ministry's most recent Military Scientific Research Report shows that fewer than 10% of the projects focus on digitalisation (15 out of 158) and fewer than 4% on AI. Instead, all AI projects are exclusively defensive in nature and focused on health, ISR and other tasks rather than enhanced warfighting capacity.[231] This is rather paradoxical given the degree of scientific expertise in the fields of AI and other emerging technologies that exists in Germany. However, it is indicative of the highly politicised nature of defence investment and defence modernisation in the country.[232]

4.3.3. Further challenges

Germany will continue to be domestically challenged in its ambition to fully embrace software-defined defence in the short and medium term. Despite solid German support for NATO and EU solidarity and interoperability in security and defence, and despite the ongoing war in Ukraine, Berlin still lacks both a clear threat assessment to inform capability development and a conviction of its responsibility to defend.[233]

New German defence-innovation structures, such as the Cyber Innovation Hub and the Cyber Agency, do not have sufficient organisational and bureaucratic pull, financial strength or embeddedness with end users to drive ambitious innovation agendas and projects, even if their capacity and knowledge base is reasonably solid.

Overcoming historical legacies and a risk-averse and overly bureaucratic organisational culture in the Ministry of Defence will remain a severe challenge, as shown by recent issues around the procurement of equipment as part of the EUR100bn (USD109bn) fund. At stake is not just the absorption of the one-time EUR100bn (USD109bn) fund, which depends on deep reforms in Germany's defence-procurement framework, but also ensuring a balanced approach between off-the-shelf purchases that deliver new equipment quickly, an understandable impulse to spend on domestic and European industrial capacity, and increasing investment in defence R&D, including greater investment in emerging technologies.[234] Longer-term German prospects for embracing a genuine software-defined defence approach depend on a shift away from current ossified procurement practices to deliver new functionality faster to the warfighter.

Moreover, German defence experts have expressed concerns that the country's defence establishment is too focused on digitalisation (digital and cyber innovation) at the expense of other critical components of future warfare, notably robotics and automation, and a more flexible approach to software-defined capabilities.[235]

Germany's coalition government has announced an intention 'to initiate a streamlining of public procurement law' to simplify and accelerate defence procurement or exempt key technologies, including advanced digital technologies, from complying with Germany's strict public-procurement law.[236]

However, there is currently no indication that Germany is moving away from very lengthy capability-development and procurement programmes or that it is pursuing more agile and iterative software development and integration projects, as recently exemplified by its participation in the F-35, THeMIS tactical UGV and FCAS programmes. This is partially explained by the fact that Germany, to a greater degree than France, is still attempting to fill historical capability gaps, rather than thinking dynamically about modern warfare and how its armed forces can credibly deter, fight and win.

5. Conclusion

The research that underpins this report focused on three core tasks. Firstly, it aimed to conceptualise software-defined defence as an emerging yet fundamental architectural, organisational and operational principle of modern military operations. It explored the transformational role of data, software and AI/ML in defence applications today and in the near future. In doing so, the paper explored four underpinning elements of a software-defined defence approach: a changing relationship between military software and hardware that means technological progress is faster in software and the promise of operational advantage in information superiority is underpinned by software-defined functionality of systems; a data-centric approach to developing and architecting new capabilities and systems-of-systems; a human-centric approach to API-enabled end-to-end electronic workflows that is designed to enhance human capacity and safety; and software as a core consideration for weapon and system design and upgrade.

Secondly, the paper sought to assess current challenges in developing and deploying modern, AI-based defence software in five case-study countries – China, France, Germany, the UK and the US. While there are incipient efforts to integrate agile and iterative software-defined defence models, particularly in France, the UK and the US, these are far from generalised. Most defence software and AI applications are developed through traditional waterfall models of capability development as an added layer to military hardware, despite these applications in some cases controlling over 80% of the capability's functionality and performance. Software is very often considered a moderate or critical risk to capability programmes. Furthermore, the structure of defence-procurement contracts and property rights continues to pose significant challenges when migrating defence software to modular and open architectures, and for the development and integration of AI applications. Most deployed or in-development defence software in France, the UK and US is customised or hardware-embedded, which means it cannot be easily upgraded without simultaneous hardware upgrades. This limits defence establishments' data rights in using the software, retrofitting legacy systems with new software solutions, and upgrading the capability frequently for increased functionality. Some examples of core common operating systems are beginning to emerge each of the three countries, but they remain the exception rather than the rule. There is no TankOS or FighterOS on the horizon at the moment, as defence software remains highly fragmented and often lacking interoperability with other service, national or allied systems.

Lastly, the research explored in detail the national efforts of the five case-study countries – China, France, Germany, the UK and the US – towards software-defined defence. It found that the intensifying strategic competition between the US and China is accelerating the transition towards software-defined defence in the two countries. However, both the US and China continue to encounter significant challenges in their efforts to achieve superiority over the other in the domain of software-defined capabilities. Yet, despite these challenges, Beijing's sustained efforts towards the digitalisation and intelligentisation of defence means the West's competitiveness advantage in software-defined defence is narrowing. The United States' advantage is increasingly confined to discrete areas (e.g., financial, technology, net organisational power and adoption patterns).

Nevertheless, the US and China remain ahead of France, Germany and the UK, whose efforts towards implementing software-defined defence have been more modest. The UK and France foster a greater level of ambition than Germany towards the digitalisation of their armed forces and the incorporation of advanced technologies like AI for operational and information advantage. London and Paris have developed the strategies, organisational structures and financial tools to pursue a software-defined defence approach. However, the use of agile and iterative software development remains too timid in both cases. France and the UK are therefore still in the early stages of a transition to software-defined defence, lacking a firm commitment to this transformation for a combination of bureaucratic, organisational-culture, financial and industrial reasons.

By contrast, there are no indications that Germany is embracing a software-defined defence approach. Instead, Berlin's capability-development plans and procurement frameworks remain ossified around long-term waterfall development models and off-the-shelf procurement of proprietary systems incorporating bespoke software linked to proprietary hardware. Efforts towards achieving digitalisation of defence and adopting a data-centric approach are slow and easily bogged down in bureaucratic procedures.

While software-defined defence entails a focus on horizontal hyperscaling of infrastructure, functionality and performance, defence establishments that are natural vertical hyperscalers in conventional military capabilities continue to struggle as microscalers of software-enabled defence.

As the European continent is shaken by high-intensity conventional war in Ukraine, early lessons from the battlefield suggest the importance of flexible approaches to the integration of innovative software solutions. China, the UK, the US and France are closely watching the developments on the battlefield and drawing insights for the future of high-intensity inter-state war. The war has spurred another wave of interest in defence investment across Europe, in NATO and the EU as well as in all three of the European nations analysed here. Berlin, however, continues to face substantial challenges in adapting, more so than any of the other nations discussed here.

There are clearly similar challenges to transitioning to software-defined defence both in the US and in Europe. However, they remain a higher barrier to entry for the Europeans. Digitalisation of defence is more expensive in Europe than in the US because of the high level of fragmentation of military equipment and entrenched defence-industrial interests around proprietary hardware and software. Beyond the siloed data, European defence ecosystems still lack fundamental building blocks for software-defined defence, including a solid governance of AI-enabled autonomy, robust enabling infrastructure and better leverage of alternative sources of funding (e.g., capital markets).

This report finds that a transatlantic gap in software-defined defence (capability and doctrinal/operational) has already emerged. Compared to the Europeans, the US is more advanced in the technological, funding, planning, experimental and doctrinal aspects of software-defined defence. US software-defined defence is and will remain much more scalable and better funded than European efforts. However, the mounting challenges in the United States' adoption of AI/ML in defence mean the transatlantic gap is relatively narrow, despite the scale and speed of US efforts. Therefore, it is our assessment that the transatlantic software-defined capabilities gap is still bridgeable in the medium to long term if the Europeans accelerate their efforts and muster the political will to fund the development of modern defence capabilities. The lessons learned from the ongoing war in Ukraine could be an important catalyst for this transformation.

Notes

[1] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York, NY: Hachette, 2020), p. 61.

[2] Mark E. Nissen, 'JSOW Alpha Contracting Case Study (Software Version)', US Naval Postgraduate School, 1997, https://man.fas.org/dod-101/sys/smart/docs/jsowcase.htm.

[3] Andrew Philip Hunter, Schuyler Moore and Maura Rose McQuade, 'Acquisition of Software-defined Hardware-based Adaptable Systems', Center for Strategic and International Studies, 7 August 2019, p. 4, https://www.csis.org/analysis/acquisition-software-defined-hardware-based-adaptable-systems.

[4] See, for example, Nand Mulchandani and Lt. General (Ret.) John N.T. 'Jack' Shanahan, 'Software-defined Warfare: Architecting the DOD's Transition to the Digital Age', Center for Strategic and International Studies, 6 September 2022, https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age; and Jason Weiss and Dan Patt, 'Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era', Hudson Institute, December 2022, https://s3.amazonaws.com/media.hudson.org/Software+Defines+Tactics.pdf.

[5] Nissen, 'JSOW Alpha Contracting Case Study (Software Version)'.

[6] National Research Council, 'Critical Code. Software Producibility for Defense', 2010, p. 19, https://apps.dtic.mil/dtic/tr/fulltext/u2/a534043.pdfhttps://apps.dtic.mil/dtic/tr/fulltext/u2/a534043.pdf.

[7] Source lines of code (SLOC) are a common measure for assessing the size of defence software used by France, Germany, the UK and the US. According to the Naval Postgraduate School's 'Software Cost Estimation Metrics Manual for Defense Systems' manual, SLOC are 'logical source statements consisting of data declarations and executables' which can be classified into new, adapted (reused, modified), equivalent, generated, converted and commercial off-the-shelf software. The latter forms the basis for cost assessments for software-development contracts in the defence establishment. See Bradford Clark and Raymond Madachy (eds.), *Software Cost Estimation Metrics Manual for Defense Systems*, (Haymarket, VA: Software Metrics Inc., 2015), pp. 19–20, http://www.softwarecost.org/Software%20Cost%20Estimation%20Metrics%20Manual%20for%20Defense%20Systems.pdf.

[8] Christian Hagen et al., 'Software: The Brains Behind U.S. Defense Systems', ATKearney, 2012, p. 2, http://ael.chungbuk.ac.kr/ael/ref/military_technologies/software/hagen(xx)-Software-The_Brains_Behind_US_Defense_Systems.pdf.

[9] Richard Hanna et al., 'Innovation Timelines from Invention to Maturity: A Rapid Review of the Evidence on the Time Taken for New Technologies to Reach Widespread Commercialisation', UK Energy Research Centre, December 2015, p. xvi, https://d2e1qxpsswcpgz.cloudfront.net/uploads/2020/03/innovation-timescales-working-paper-march-2016.pdf.

[10] Author interview with former military official, July 2022.

[11] Megan Eckstein, 'Navy's Digital Horizon exercise showcases power of "mesh networks," AI', *C4ISRNET*, 14 December 2022, https://www.c4isrnet.com/naval/2022/12/14/navys-digital-horizon-exercise-showcases-power-of-mesh-networks-ai/.

[12] Craig Fields et al., 'Design and Acquisition of Software for Defense Systems', US Department of Defense, Defense Science Board (DSB), 14 February 2018, pp. 3 and 23, https://apps.dtic.mil/sti/pdfs/AD1048883.pdf.

[13] Simona R. Soare, 'Cooperative Edge: Key Drivers of Defence Innovation in Multilateral Organisations Like the EU and NATO', IISS research paper, forthcoming 2023.

[14] Emmanuel Huberdeau, 'Geospatial intelligence: Earthcube promotes automated imagery analysis', *Jane's International Defence Review*, 18 November 2019.

[15] Ted Johnson and Charles F. Wald, 'The Military Should Teach AI to Watch Drone Footage', *Wired*, 26 November 2017, https://www.wired.com/story/the-military-should-teach-ai-to-watch-drone-footage/.

[16] US Government Accountability Office, 'Battle Management: DOD and Air Force Continue to Define Joint Command and Control Efforts', GAO-23-105495, January 2023, p. 18, https://www.gao.gov/assets/820/814635.pdf.

[17] *Ibid*, p. 9.

[18] German Federal Ministry of Defence, 'Information from the Parliamentary Commissioner for the Armed Forces: Annual Report 2020 (62nd Report)', 23 February 2021, p. 93, https://www.bundestag.de/resource/blob/839328/e1a864120697c27057534944ceb20111/annual_report_2020_62nd_report-data.pdf.

19 Examples include the digital systems onboard Germany's *Tornado* multirole fighter aircraft, key DoD network enterprise systems and C2 and mission-planning tools still running on Windows 2008 servers, and the DoD's use of eight-inch floppy disks, which have not been used commercially in over two decades, for data sharing in its nuclear forces.

20 Jed Judson, 'Project Convergence exercise has new gateway to test emerging tech', DefenseNews, 11 October 2022, https://www.defensenews.com/training-sim/2022/10/10/project-convergence-exercise-has-new-gateway-to-test-emerging-tech/.

21 IISS workshop, 'Future-proofing Defence: Opportunities and Challenges of Software-defined Defence', 7 December 2022. See also Megan Eckstein, 'Navy's Digital Horizon exercise showcases power of "mesh networks," AI'; and Jon Harper, 'Navy to Establish Additional Unmanned Task Forces Inspired by Task Force 59', Defensescoop, 4 December 2022, https://defensescoop.com/2022/12/04/navy-to-establish-additional-unmanned-task-forces-inspired-by-task-force-59/.

22 Jason Weiss and Dan Patt, 'Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era', p. 12.

23 Simona R. Soare, 'Algorithmic Power, NATO and Artificial Intelligence', IISS Military Balance Blog, 19 November 2021, https://www.iiss.org/blogs/military-balance/2021/11/algorithmic-power-nato-and-artificial-intelligence.

24 Hayley Patterson, 'From Software to Battlespace: Reimagining How Defence Does DevSecOps with D2S', Defence Digital/Digital Foundry, UK Ministry of Defence, 19 August 2022, https://defencedigital.blog.gov.uk/2022/08/19/from-software-to-battlespace-reimagining-how-defence-does-devsecops-with-d2s/.

25 National Research Council of the National Academies, 'Critical Code. Software Producibility for Defense', 2010, p. 19, https://apps.dtic.mil/dtic/tr/fulltext/u2/a534043.pdf.

26 Mulchandani and Shanahan, 'Software-defined Warfare: Architecting the DOD's Transition to the Digital Age', p. 6.

27 *Ibid*, p. 11.

28 US Navy, 'Software Ecosystem Architectural Model and Application Program Interface for Common Core Combat System', Navy SBIR 2020.1 – Topic N201-057, 14 January 2020, https://www.navysbir.com/n20_1/N201-057.htm.

29 Mulchandani and Shanahan, 'Software-defined Warfare: Architecting the DOD's Transition to the Digital Age', p. 10.

30 IISS workshop, 'Future-proofing Defence: Opportunities and Challenges of Software-defined Defence'.

31 Dassault Aviation, 'Launch of the Man Machine Teaming Advanced Study Programme', 16 March 2018, https://www.dassault-aviation.com/en/group/press/press-kits/launch-man-machine-teaming-advanced-study-programme/; and Airforce Technology, 'France launches Man-Machine-Teaming Programme to Develop AI for Combat Aviation', 20 March 2018, https://www.airforce-technology.com/news/france-launches-man-machine-teaming-programme-develop-ai-combat-aviation/.

32 The available open-source information regarding Chinese capability-development practices in general, and software-development practices in particular, is insufficient to substantiate a clear determination and assessment as in the case of the four Western case studies investigated here.

33 The waterfall capability-development model is the most commonly used framework for major capability programmes across the five case-study countries studies analysed in this paper. It has been the predominant framework for capability development since the 1970s, and relies on strict, linear and interconnected phases in which previous phases must be successfully completed before proceeding to the next phase. The phases of a waterfall model include definition of requirements, design, execution, testing and release. By contrast, agile models build on small increments of the capability requirements and enable a continuous integration/continuous delivery approach. Other models include incremental, spiral, agile, DevOps, and hybrid or mixed. For a comprehensive definition of these capability-development models and how they apply to software, see US Governmental Accountability Office, 'DoD Software Acquisition: Status of and Challenges Related to Reform Efforts', GAO-21-105298, September 2021, p. 4, https://www.gao.gov/assets/gao-21-105298.pdf.

34 US Government Accountability Office, 'Report to Congressional Committees: Weapon Systems Annual Assessment. Challenges to Fielding Capabilities Faster Persist', June 2022, https://www.gao.gov/assets/gao-22-105230.pdf.

35 These include emerging and emergent technology stacks in AI/ML, data science, quantum, space, next-generation (tele)communication, biotechnology, human enhancement, directed energy, new propulsion systems, advanced manufacturing, additive materials and more.

36 See, for example, a comprehensive list of US Department of Defence recommendations on adapting software development practices since the late 1980s in Defence Innovation Board,

'Software Acquisition and Practices (SWAP) Study', May 2019, pp. 19–21, https://innovation.defense.gov/software/.

37 See, for example, Leonardo, 'Leonardo Accelerates the Digitalization of the Aerospace Defence and Security Sector. Genoa Is the National Industrial Competence Hub', 1 December 2021, https://www.leonardo.com/en/press-release-detail/-/detail/01-12-2021-leonardo-accelerates-the-digitalization-of-the-aerospace-defence-and-security-sector.

38 Steven Rosenbush, 'Big Tech Is Spending Billions on AI Research. Investors Should Keep an Eye Out', *Wall Street Journal*, 8 March 2022, https://www.wsj.com/articles/big-tech-is-spending-billions-on-ai-research-investors-should-keep-an-eye-out-11646740800.

39 See, for example, Macrotrends, 'Palantir Technologies Research and Development Expenses 2019-2022 | PLTR', 2022, https://www.macrotrends.net/stocks/charts/PLTR/palantir-technologies/research-development-expenses.

40 GlobalData, 'Top Big Data Patent Holders in the Aerospace and Defence Sector (2002-2022)', November 2022, https://www.globaldata.com/data-insights/aerospace-and-defence/global-top-big-data-patents-holders-in-the-aerospace-and-defence-sector-2131090/.

41 Aerospace, Security and Defence Industries Association of Europe (ASD), '2022 Facts & Figures', 2022, pp. 21–23, https://asd-europe.paddlecms.net/sites/default/files/2022-11/ASD_Facts%20%26%20Figures%202022.pdf.

42 Statista, 'Expenditure on Research and Development of Defense Technology Supplier Lockheed Martin from 2002 to 2021', January 2023, https://www.statista.com/statistics/268928/expenditure-on-research-and-development-of-defense-supplier-lockheed-martin/.

43 US Government Accountability Office, 'F35 Joint Strike Fighter: Cost Growth and Schedule Delays Continue, Statement of Jon Ludwigson, Director, Contracting and National Security Acquisitions', GAO-22-105943, 27 April 2022, pp. 10–12, https://www.gao.gov/assets/730/720256.pdf; and US Government Accountability Office, 'F35 Joint Strike Fighter: DOD Needs to Update Modernization Schedule and Improve Data on Software Development', GAO-21-226, March 2021, p. 28, https://www.gao.gov/assets/720/713140.pdf.

44 US Government Accountability Office, 'Tactical Aircraft: F-22A Modernization Program Faces Cost, Technical, and Sustainment Risks', GAO-12-447, May 2012, p. 6, https://www.gao.gov/assets/gao-12-447.pdf.

45 Niall McCarthy, 'The Mammoth Cost of Operating America's Combat Aircraft', *Forbes*, 26 November 2020, https://www.forbes.com/sites/niallmccarthy/2020/11/26/the-mammoth-cost-of-operating-americas-combat-aircraft-infographic/?sh=3e26f1e87da7.

46 Simona R. Soare and Fabrice Pothier, 'Leading Edge: Key Drivers of Defence Innovation and the Future of Operational Advantage', IISS, 11 November 2021, p. 23, https://www.iiss.org/blogs/research-paper/2021/11/key-drivers-of-defence--innovation-and-the-future--of-operational-advantage.

47 Fields et al., 'Design and Acquisition of Software for Defense Systems', pp. 1–2.

48 *Ibid*.

49 Shephard Media, 'Rheinmetall Joins Helsing to Accelerate AI for Land Systems', 15 September 2022, https://www.shephardmedia.com/news/digital-battlespace/rheinmetall-joins-helsing-to-accelerate-ai-for-land-systems/.

50 Palantir, 'Palantir Announces Availability of Foundry on Microsoft Azure', Palantir Blog, 25 January 2023, https://blog.palantir.com/palantir-announces-availability-of-foundry-on-microsoft-azure-9120311e2d1a.

51 Atos, 'AWS and Atos Strengthen Collaboration with New Strategic Partnership to Transform the Infrastructure Outsourcing Industry', 30 November 2022, https://atos.net/en/2022/press-release_2022_11_30/aws-and-atos-strengthen-collaboration-with-new-strategic-partnership-to-transform-the-infrastructure-outsourcing-industry.

52 Office of the Under Secretary of Defense (Comptroller), 'RDT&E Programs (R-1)', April 2022, p. iii, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_r1.pdf; and US Government Accountability Office, 'Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance', GAO-22-105834, March 2022, p. 2, https://www.gao.gov/assets/gao-22-105834.pdf.

53 Douglas Barrie, Nick Childs and Fenella McGerty, 'US FY2023 defence budget request: something old, something new…', IISS Military Balance Blog, 14 April 2022, https://www.iiss.org/blogs/military-balance/2022/04/us-fy2023-defence-budget-request-something-old-something-new.

54 Margarita Konaev et al., 'US Military Investments in Autonomy and AI: A Budgetary Assessment', Center for Security and Emerging Technology, October 2020, pp. 15–18, https://cset.georgetown.edu/wp-content/uploads/CSET-U.S.-Military-Investments-in-Autonomy-and-AI-A-Budgetary-Assessment-1.pdf; and Chris Cornillie, 'Artificial Intelligence

& Machine Learning: BGOV Market Profile', Bloomberg Government, 23 September 2020, https://about.bgov.com/reports/market-profile-artificial-intelligence-and-machine-learning/.

55 Authors' calculations based on Office of the Under Secretary of Defense (Comptroller), 'RDT&E Programs (R-1)'. This estimate is based on the enacted FY22 and requested FY23 funding for military services and DoD-wide projects in which AI/ML either represents a key deliverable, a critical component of the deliverable or in which AI/ML is used in a prominent role in the development process. We recognise the definitional problem where definitions of AI/ML are still inconsistent across services and the DoD.

56 *Ibid*.

57 Govini, 'The National Security Scorecard: Critical Technologies Edition', 29 June 2022, p. 4, https://govini.com/wp-content/uploads/2022/06/Govini-National-Security-Scorecard-Critical-Technologies.pdf.

58 *Ibid*, p. 21.

59 Ashwin Acharya and Zachary Arnold, 'Chinese Public AI R&D Spending: Provisional Findings', Center for Security and Emerging Technology Issue Brief, December 2019, p. 13, https://cset.georgetown.edu/publication/chinese-public-ai-rd-spending-provisional-findings/.

60 Ryan Fedasiuk, Jennifer Melot and Ben Murphy, 'Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence', Center for Security and Emerging Technology, October 2021, p. 10, https://cset.georgetown.edu/publication/harnessed-lightning/.

61 Acharya and Arnold, 'Chinese Public AI R&D Spending: Provisional Findings', p. 2.

62 IISS workshop, 'Future-proofing Defence: Opportunities and Challenges of Software-defined Defence'.

63 Fedasiuk, Melot and Murphy, 'Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence', pp. 7–8 and 10.

64 HM Government, 'Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy', 16 March 2021, p. 38, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf; see also Ministry of Defence, 'Ministry of Defence's Science and Technology Portfolio', of Defence's Science and Technology portfolio,' updated 23 January 2023, https://www.gov.uk/government/publications/defence-science-and-technology-programmes-and-projects/ministry-of-defences-science-and-technology-portfolio.

65 HM Treasury, 'Budget 2020: Delivering on Our Promises to the British people', 11 March 2020, p. 85, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/871799/Budget_2020_Web_Accessible_Complete.pdf.

66 UK National Audit Office, 'The Equipment Plan 2022 to 2032', 29 November 2022, p. 18, https://www.nao.org.uk/wp-content/uploads/2022/11/NAO-Report-The-equipment-plan-2022-to-2032.pdf.

67 Based on UK MoD software services tenders between January–December 2022 listed in Bidstats. For more details, see https://bidstats.uk/tenders/?ntype=tender#792330239-792068335-47.

68 UK National Audit Office, 'The Digital Strategy for Defence: A Review of Early Implementation', 19 October 2022, p. 2, https://www.nao.org.uk/wp-content/uploads/2022/10/NAO-report-The-Digital-Strategy-for-Defence-A-review-of-early-implementation.pdf.

69 *Ibid*.

70 UK Ministry of Defence, 'Annual Report and Accounts 2021–22', 14 July 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1090612/20220714_MOD-ARA_2021-22.pdf.

71 UK National Audit Office, 'The Digital Strategy for Defence: A Review of Early Implementation', p. 29.

72 *Ibid*, p. 32.

73 France24, 'France to Invest €1.5 Billion in Artificial Intelligence by 2022', 29 March 2018, https://www.france24.com/en/20180329-france-invest-15-billion-euros-artificial-intelligence-AI-technology-2022.

74 See Ministère des Armées, 'Projet de Loi de Finances 2023 : Loi de Programmation Militaire 2019–2025', 2023, p. 28, https://www.defense.gouv.fr/sites/default/files/ministere-armees/Projet%20de%20loi%20de%20finances%20-%202023%20-%20LPM%20année%205.pdf; Assemblée Nationale, 'Avis Fait au Nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de la Loi de Finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense', par M. Fabien Gouttefarde, Député, 20 October 2021, https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b4601-tii_rapport-avis#_Toc256000032; and Agence d'Innovation de Défense, 'Innovation de Défense: Bilan d'Activités 2021',

2022, https://www.defense.gouv.fr/sites/default/files/aid/Bilan%20d%27activités%202021.pdf.

75 Vivienne Machi, 'France Approves Final Phase of Artemis Big-data Processing Platform', DefenseNews, 11 July 2022, https://www.defensenews.com/global/europe/2022/07/11/france-approves-final-phase-of-artemis-big-data-processing-platform/.

76 Assemblée Nationale, 'Avis Fait au Nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de la Loi de Finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense', par M. Fabien Gouttefarde, Député.

77 *Ibid*.

78 *Ibid*.

79 Laurent Lagneau, 'Renseignement: Le ministère des Armées lance le projet TORNADE pour le traitement massif des données', *Opex360.com*, 12 October 2022, https://www.opex360.com/2022/10/12/renseignement-le-ministere-des-armees-lance-le-projet-tornade-pour-le-traitement-massif-des-donnees/.

80 Vivienne Machi, 'French 2023 defense budget adds $3 billion to fund "war economy"', DefenseNews, 28 September 2022, https://www.defensenews.com/global/europe/2022/09/28/french-2023-defense-budget-adds-3-billion-to-fund-war-economy/.

81 Agence d'Innovation de Défense, 'Innovation de Défense Bilan d'Activités 2021', p. 12.

82 Lagneau, 'Renseignement: Le ministère des Armées lance le projet TORNADE pour le traitement massif des données'. See also Earthcube, 'Press Release: Series-A and Name Change', 19 November 2020, https://www.preligens.com/resources/press/press-release-series-name-change.

83 Bastian Giegerich and Ben Schreer, 'Germany's New Defence Policy: The 100 Billion Euro Question', IISS Military Balance Blog, 1 March2022,https://www.iiss.org/blogs/military-balance/2022/03/germanys-new-defence-policy-the-100-billion-euro-question.

84 German Ministry of Defence, 'Defence Budget 2021', December 2020, https://www.bmvg.de/de/themen/verteidigungshaushalt/verteidigungshaushalt-2021. See also Christian Mölling and Torben Schütz, 'Defence Innovation: New Models and Procurement Implications: The German Case', Armament Industry European Research Group, May 2021, pp. 6–7, https://www.iris-france.org/wp-content/uploads/2021/05/68-Policy-Paper-Def-Innov-German-Case-May-2021.pdf.

85 German Federal Ministry of Finance, 'Discover the Federal Budget Interactively: Federal Ministry of Defence 2023', December 2022, https://www.bundeshaushalt.de/DE/Bundeshaushalt-digital/bundeshaushalt-digital.html.

86 Lisa Daigle, 'German Companies Team for Digitization of Germany's Ground Forces', 27 March 2017, https://militaryembedded.com/comms/communications/german-companies-team-for-digitization-of-germanys-ground-forces.

87 See, for example, Thales Group, 'D-LBO (Digital Landbased Operations)' and 'TEN (Tactical Edge Networking)', 2021, https://www.thalesgroup.com/en/europe/germany/d-lbo-ten; and Systematic, 'C4I Software for the Digitalisation of the German Army', 10 March 2022, https://systematic.com/en-gb/industries/defence/news-knowledge/news/2022_c4i-across-the-german-armed-forces/.

88 Peter Hille and Nina Werkhäuser, 'The German military's new shopping list', DW, 6 March 2022, https://www.dw.com/en/how-will-the-german-military-spend-100-billion/a-62020972.

89 US Air Force, 'AFVentures: FY18-FY20 Impact Report', 2021, p. 2, https://afwerx.com/wp-content/uploads/2021/10/AFVentures-2020-Annual-Report.pdf.

90 Simona R. Soare, 'European Military AI: Why Regional Approaches Are Lagging Behind', in Michael Raska and Richard Bitzinger (eds.), *Global Strategic Perspectives on Military AI* (London: Routledge, forthcoming 2023).

91 Assemblée Nationale, 'Avis fait au nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de la Loi de finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense', par M. Fabien Gouttefarde, Député.

92 *Ibid* and Agence d'Innovation de Défense, 'Innovation de Défense: Bilan d'Activités 2021'.

93 Bpifrance, 'Definvest, le Fonds du Ministère des Armées géré par Bpifrance, soutient le développement de pme stratégiques de la défense', *Fusions et Acquisitions Magazine*, January–February 2019, p. 4, https://fusions-acquisitions.info/wp-content/uploads/2020/05/FA-301-3-5-1.pdf.

94 Authors' calculations based on data on overall budgets and new competitions in several US defence agencies, including the Defence Advanced Research Projects Agency (DARPA), Defence Information Systems Agency (DISA), Defence Security Cooperation Agency (DSCA), Defence Threat Reduction Agency (DTRA), Missile Defence Agency (MDA), US Special Operations Forces (SOF) and National Science Foundation (NSF), in FY 21.

95 Authors' calculations based on data on new competitions launched by the Dstl and DASA in the UK, the AID in France and the Cyber Innovation Hub in Germany between 1 June 2021–31 December 2022.

96 Simona R. Soare, 'Cooperative edge: Key Drivers of Defence Innovation in Multinational Institutions like NATO and the EU', IISS, forthcoming 2023.

97 Fields et al., 'Design and Acquisition of Software for Defense Systems', p. 3 and Patterson, 'From Software to Battlespace: Reimagining how Defence does DevSecOps with D2S'.

98 US Government Accountability Office, 'DOD Software Acquisition: Status of and Challenges Related to Reform Efforts', GAO-21-105298.

99 Fields et al., 'Design and Acquisition of Software for Defense Systems', pp. 13 and 18.

100 German Federal Ministry of Defence, 'Information from the Parliamentary Commissioner for the Armed Forces: Annual Report2020(62ndReport)',23February2021,p.94,https://www.bundestag.de/resource/blob/839328/e1a864120697c2705 7534944ceb20111/annual_report_2020_62nd_report-data.pdf.

101 The US DoD's taxonomy on software distinguishes between enterprise systems, business systems and combat systems. Enterprise systems are very large-scale software systems used at the DoD level for a variety of purposes and which rely on unmodified commercial off-the-shelf software, but with a DoD-specific configuration. Notable examples are email systems, accounting systems, travel systems and human-resources databases. Business systems are also very large-scale software systems which generally operate at agency or service level. Examples include software-development environments and logistics systems. Combat systems are unique to defence and often require at least some level of customisation. Combat systems include logistics systems (software to track materials, supplies and spare parts, transport as part of operational use), mission systems (mission planning and monitoring software systems, including modelling and simulation) and weapons systems (any software which directly engages or supports lethal force and the operation of a weapon platform). To enable greater warfighting advantage, mission and weapons systems require new software-defined functionality frequently (approximated in days to months). However, weapon-systems software is the most challenging to update regularly, as it is traditionally closely tied to hardware, one of the enduring challenges of agile and iterative approaches to software development. See US Defence Innovation Board, 'Software Acquisition and Practices (SWAP) Study', May 2019, pp. 2–3, https://media.defense.gov/2019/May/01/2002126693/-1/-1/0/SWAP%20MAIN%20REPORT.PDF.

102 Kevin Garrison, David M. Tate and John W. Bailey, 'Factors Limiting the Speed of Software Acquisition', Institute for Defence Analyses, October 2019, pp. 7–8, https://www.ida.org/-/media/feature/publications/f/fa/factors-limiting-the-speed-of-software-acquisition/d-10907.ashx.

103 US Government Accountability Office, 'Weapon Systems Annual Assessment: Challenges to Fielding Capabilities Faster Persist', GAO-22-105230, June 2022, p. 129, https://www.gao.gov/assets/gao-22-105230.pdf.

104 Author calculations based on data from Government Accountability Office, 'Report to Congressional Committees: Weapon Systems Annual Assessment. Challenges to Fielding Capabilities Faster Persist'.

105 *Ibid*, p. 93.

106 *Ibid*.

107 *Ibid*.

108 Comprehensive analysis of defence software development shortcomings in the US can be found in Office of the Undersecretary of Defense for Research and Engineering, 'Design and Acquisition of Software for Defense Systems', US Defense Science Board, 14 February 2018, https://apps.dtic.mil/sti/pdfs/AD1048883.pdf; US Government Accountability Office, 'Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems', GAO-22-10476, February 2022, https://www.gao.gov/assets/gao-22-104765.pdf; US Government Accountability Office, 'DOD Software Acquisition: Status of and Challenges Related to Reform Efforts', GAO-21-105298; and Kevin Garrison, David M. Tate and John W. Bailey, 'Factors Limiting the Speed of Software Acquisition', Institute for Defense Analyses, D-10907, October 2019, https://www.ida.org/-/media/feature/publications/f/fa/factors-limiting-the-speed-of-software-acquisition/d-10907.ashx.

109 US Department of Defense, 'Summary of the 2018 National Defence Strategy of the United States of America: Sharpening the American Military's Competitive Edge', 22 January 2018, p. 10, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

110 White House, 'National Security Strategy', 12 October 2022, p. 22, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

111 US Department of Defense, '2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defence Review', 27 October 2022, p. 19, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[112] US Department of Defense, '2019 Digital Modernization Strategy', 12 July 2019, p. 44, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

[113] US Department of Defense, 'Executive Summary: DoD Data Strategy', 30 September 2020, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

[114] US Deputy Secretary of Defense, 'Deputy Secretary of Defense Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, Defense Agency and DoD Field Activity Directors, Subject: Initial Operating Capability of the Chief Digital and Artificial Intelligence Officer', 1 February 2022, https://media.defense.gov/2022/Feb/02/2002931807/-1/-1/1/MEMORANDUM-ON-THE-INITIAL-OPERATING-CAPABILITY-OF-THE-CHIEF-DIGITAL-AND-ARTIFICIAL-INTELLIGENCE-OFFICER.PDF.

[115] Govini, 'The 2020 Federal Scorecard', 2020, p. 27, https://govini.com/research/the-2020-federal-scorecard/.

[116] *Ibid*.

[117] *Ibid*.

[118] US Department of Defense, 'Hicks Announces New Artificial Intelligence Initiative', DoD News, 22 June 2021, https://www.defense.gov/News/News-Stories/Article/Article/2667212/hicks-announces-new-artificial-intelligence-initiative/.

[119] US Government Accountability Office, 'Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapons Systems', GAO-22-104765.

[120] New York University, 'DARPA Award Aims For Autonomous Teams Of Robots', Science Blog, 29 September 2022, https://scienceblog.com/534015/darpa-award-aims-for-autonomous-teams-of-robots/.

[121] US Department of Defense, '2019 Digital Modernization Strategy'.

[122] National Security Commission on Artificial Intelligence, 'Final Report', 19 March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[123] US Congress, 'Statement of Dr. Eric Schmidt to the House Armed Services Committee', 17 April 2018, https://es.ndu.edu/Portals/75/Documents/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf.

[124] Author interview with the Department of Defense's Chief Digital and AI Officer Craig Martell, 21 October 2022.

[125] The State Council of the People's Republic of China, 'Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisi ge wu nian guihua he 2035 nian yuanjing mubiao gangyao' 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 [Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Range Goals for 2035], 13 March 2021, http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm.

[126] The State Council of the People's Republic of China, 'Guowuyuan guanyu yinfa xin yidai rengong zhineng fazhan guihua de tongzhi guo fa' 国务院关于印发新一代人工智能发展规划的通知国发 [The State Council on Issuance of the Development Plan for the New Generation of Artificial Intelligence], No. 35, 20 July 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

[127] Li Changhai 李长海, Han Jian 韩剑 and Zhu Hao 朱昊, 'Yong shuju shuohua de shidai, da shuju ruhe tuijin zhuangbei baozhang biange' 用数据说话的时代，大数据如何推进装备保障变革 [In the Era of Using Data, How Can Big Data Advance Equipment Security Changes], *PLA Daily*, 7 July 2020, http://www.81.cn/jmywyl/2020-07/07/content_9847982.htm.

[128] Song Yuangang 宋元刚, Shao Longfei 邵龙飞 and Wang Han 特约记者 王晗, 'Junshi da shuju: Junshi zhineng biange de jiasuqi' 军事大数据：军事智能变革的加速器 [Military Big Data: An Accelerator of Change for Military Intelligence], *PLA Daily*, 6 September 2019, http://www.81.cn/bqtd/2019-09/06/content_9632838.htm.

[129] The State Council of the People's Republic of China, 'Xi Jinping: Gaoju zhongguo tese shehui zhuyi weida qizhi wei quanmian jianshe shehui zhuyi xiandaihua guojia er tuanjie fendou—zai zhongguo gongchandang de ershi ci quanguo daibiao dahui shang de baogao' 习近平：高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告 [Xi Jinping: Holding High the Great Banner of Socialism with Chinese Characteristics and Uniting the Struggle for the Comprehensive Construction of a Modern Socialist Country - Report at the 20th National Congress of the Communist Party of China], 25 October 2022, http://www.gov.cn/zhuanti/zggcddescqgdbdh/sybgqw.htm.

[130] The State Council of the People's Republic of China, 'National New Generation AI Plan', The OECD Artificial Intelligence Policy Observatory, 5 September 2022, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24274, https://oecd.ai/en/dashboards/policy-initiatives/http://aipo.oecd.org/2021-data-policyInitiatives-24274.

[131] Acharya and Arnold, 'Chinese Public AI R&D Spending: Provisional Findings'.

132 Yuangang, Longfei and Han, 'Junshi da shuju: Junshi zhineng biange de jiasuqi' 军事大数据：军事智能变革的加速器 [Military Big Data: An Accelerator of Change for Military Intelligence].

133 FBI, 'Chinese Military Hackers Charged in Equifax Breach', 10 February 2020, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020.

134 Matt Pottinger and David Feith, 'The Most Powerful Data Broker in the World Is Winning the War Against the U.S.', *New York Times* opinion piece, 30 November 2021, https://www.nytimes.com/2021/11/30/opinion/xi-jinping-china-us-data-war.html.

135 Wu Min 吴敏, Chen Fengjun 陈凤军 and Zhang Dan 张丹, 'Shenhua da shuju jishu zai junshi lingyu de yingyong' 深化大数据技术在军事领域的应用 [Deepen the Application of Big Data Technology in the Military Field], *PLA Daily*, 2 March 2021, http://www.81.cn/jfjbmap/content/2021-03/02/content_283870.htm.

136 School of Shipbuilding, 'Zhongguo shou ge shi haikuang zhineng chuan ting jingsai zai shanghai jiaoda haiyang zhuangbei zhineng yanjin zhongxin juban' 中国首个实海况智能船艇竞赛在上海交大海洋装备智能演进中心举办 [China's first real-sea intelligent boat competition was held at Shanghai Jiaotong University Marine Equipment Intelligent Evolution Centre], Shanghai Jiaotong University, 15 October 2019, https://news.sjtu.edu.cn/jdyw/20191014/112627.html.

137 Cyberspace Administration of China, 'Yi zhi zhangyu gaibianle wangluo anquan youxi guize' 只章鱼改变了网络安全游戏规则 [An Octopus Changed the Rules of the Cybersecurity Game], *Science and Technology Daily*, 28 May 2019, http://www.cac.gov.cn/2019-05/28/c_1124549858.htm.

138 Yang Wei, 'Development of future fighters', *Acta Aeronautica et Astronautica Sinica*, vol. 41, no. 6, June 2020, pp. 8–19.

139 Ministry of Foreign Affairs of the People's Republic of China, 'Zhongguo guanyu guifan rengong zhineng junshi yingyong de lichang wenjian' 中国关于规范人工智能军事应用的立场文件 [China's Position Paper on Regulating Military Applications of Artificial Intelligence], 14 December 2021, https://www.fmprc.gov.cn/web/wjb_673085/zfxxgk_674865/gknrlb/tywj/zcwj/202112/t20211214_10469511.shtml.

140 Tai Ming Cheung, 'Strengths and Weaknesses of China's Defense Industry and Acquisition System and Implications for the United States', Naval Postgraduate School, Acquisition Research Program Sponsored Report Series, 25 June 2018, https://dair.nps.edu/bitstream/123456789/2724/1/UCSD-AM-18-218.pdf.

141 Andrea Gilli and Mauro Gilli, 'Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', *International Security*, vol. 43, no. 3, Winter 2018/2019, pp. 141–189.

142 Elsa B. Kania, '"AI Weapons" in China's Military Innovation', Brookings Institution, *Global China: Assessing China's Growing Role in the World*, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf.

143 Bureau of Industry and Security, 'Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification', Federal Register, vol. 87, no. 197, 13 October 2022, https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor; and Nigel Inkster, Emily S. Weinstein and John Lee, 'Ask the Experts: Is China's Semiconductor Strategy Working?', LSE Blogs, 1 September 2022, https://blogs.lse.ac.uk/cff/2022/09/01/is-chinas-semiconductor-strategy-working/.

144 Mathieu Duchâtel, 'The Weak Links in China's Drive for Semiconductors', Institute Montaigne Policy Paper, January 2021, https://www.institutmontaigne.org/en/publications/weak-links-chinas-drive-semiconductors.

145 Che Pan, 'Tech War: Beijing, Local Governments Pressed to Raise Support for Chinese Chip Research and Development Amid US Expansion', *South China Morning Post*, 26 August 2022, https://www.scmp.com/tech/tech-war/article/3190323/tech-war-beijing-local-governments-pressed-raise-support-chinese-chip.

146 Science and Technology News, 'Nvidia Makes New "Advanced" AI Chip for China That Meets Trade Restrictions', 8 November 2022, https://www.technology.org/2022/11/08/nvidia-makes-new-advanced-ai-chip-for-china-that-meets-trade-restrictions/.

147 Inkster, Weinstein and Lee, 'Ask the Experts: Is China's Semiconductor Strategy Working?'.

148 Pan, 'Tech War: Beijing, Local Governments Pressed to Raise Support for Chinese Chip Research and Development Amid US Expansion'.

149 For an in-depth analysis of the relationship between national defence AI/ML capability development and multinational initiatives within NATO and the EU see Simona R. Soare, 'European Military AI: Why Regional Approaches are Lagging Behind'.

150 Author interview with former French defence official, 2022.

151 Tom Copinger-Symes, 'For National Defence, a Digital Arsenal Is Now Vital', *Wired*, 18 February 2022, https://www.wired.co.uk/article/national-defence-digital-warfare.

152 Soare and Pothier, 'Leading Edge: Key Drivers of Defence Innovation and the Future of Operational Advantage'.

153 UK Ministry of Defence, 'The Defence Capability Framework', 6 July 2022, https://www.gov.uk/government/publications/the-defence-capability-framework.

154 UK Ministry of Defence, 'Integrated Operating Concept', August 2021, p. 7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf.

155 UK Ministry of Defence, 'Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data', 27 September 2021, p. 11, https://www.gov.uk/government/publications/data-strategy-for-defence.

156 UK Ministry of Defence, 'Digital Strategy for Defence: Delivering the Digital Backbone and Unleashing the Power of Defence's Data', 27 May 2021, p. 10, https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data.

157 UK Ministry of Defence, 'Ambitious, Safe, Responsible: Our Approach to the Delivery of AI-enabled Capability in Defence', June 2022, p. 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082991/20220614-Ambitious_Safe_and_Responsible.pdf.

158 UK Ministry of Defence, 'Defence Artificial Intelligence Strategy', June 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082416/Defence_Artificial_Intelligence_Strategy.pdf.

159 *Ibid*, p. 1.

160 *Ibid*, p. 2.

161 UK National Audit Office, 'The Digital Strategy for Defence: A Review of Early Implementation', pp. 8–10 and 27.

162 IISS, 'Defence Innovation Talks: a Conversation with General Sir Nick Carter', 30 March 2021, https://www.iiss.org/events/2021/03/defence-innovation-talks-general-sir-nick-carter.

163 UK Ministry of Defence, 'Joint Doctrine Note 1/23: Intelligence, Surveillance and Reconnaissance', January 2023, pp. 65–69, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1130778/JDN_1_23_ISR_web.pdf.

164 UK Ministry of Defence, 'MOD Awards £3.8-million Contract for Advanced Base Protection System', 10 September 2021, https://www.gov.uk/government/news/mod-awards-38-million-contract-for-advanced-base-protection-system.

165 Kenneth Payne, 'Bright Prospects – Big Challenges: Defence AI in the United Kingdom', Defence AI Observatory, 2022, pp. 15–16, https://defenseai.eu/wp-content/uploads/2023/01/DAIO_Study2204.pdf.

166 The Stack, 'UK's Ministry of Defence Signs £75m Deal with Palantir', 22 December 2022, https://thestack.technology/uk-ministry-of-defence-palantir-contract-mod/.

167 UK Ministry of Defence, 'MOD Awards £3.8-million Contract for Advanced Base Protection System'.

168 Royal Navy, 'New Testbed Ship to Enhance Experimentation in Royal Navy', 29 July 2022, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/july/29/20220729-new-testbed-ship-to-enhance-experimentation-in-royal-navy.

169 Olivia Savage, 'DTDT 2022: Royal Navy Official Calls for New Experimentation Facility', *Janes Defence Weekly*, 30 September 2022, https://www.janes.com/defence-news/news-detail/dtdt-2022-royal-navy-official-calls-for-new-experimentation-facility.

170 Royal Navy, 'Royal Marines Take Big Step With New Technology', 25 April 2019, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2019/april/25/190425-commando-warrior.

171 Patterson, 'From Software to Battlespace: Reimagining how Defence does DevSecOps with D2S'.

172 Author interview with defence official, July 2022.

173 UK Army, 'Project Convergence 22: What is Sensor-Decider-Effector?', 31 October 2022, https://www.army.mod.uk/news-and-events/news/2022/10/project-convergence-22-sensor-decider-effector/.

174 Royal Navy, 'New London Innovation Hub Will See Royal Navy and US Navy Embrace Technology Together', 14 June 2022, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/june/14/220614-london-tech-bridge-launch.

175 Royal Air Force, 'RAF FP Force Supporting Innovative Ways To Provide Force Protection', 18 November 2021, https://www.raf.mod.uk/our-organisation/force-protection/news/raf-fp-force-supporting-innovative-ways-to-provide-force-protection/.

176 Jamie Grierson, 'MoD Delivery of Ajax Armoured Vehicles will be a Challenge, says Watchdog', *Guardian*, 11 March 2022, https://www.theguardian.com/uk-news/2022/mar/11/mod-delivery-of-ajax-armoured-vehicles-will-be-a-challenge-says-watchdog; and UK National Audit Office, 'The Ajax Programme', 11 March 2022,

https://www.nao.org.uk/wp-content/uploads/2022/03/The-Ajax-programme.pdf.

177 NASA, 'Storm Clouds over Stonehenge: UK Watchkeeper UAS Mishap', *NASA Safety Center*, System Failure Case Study, vol 19, issue 1, April 2019, https://www.scribd.com/document/485908721/Storm-Clouds-Over-Stonehenge#.

178 UK National Audit Office, 'The Equipment Plan 2022 to 2032', p. 8.

179 Author interview with defence representatives, September 2022.

180 Ministère des Armées, 'Artificial Intelligence in Support of Defence: Report of the AI Task Force', September 2019, p. 5, https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf.

181 Ministère des Armées, 'Strategic Update 2021: Synthesis', 2021, https://s.rfi.fr/media/display/e19540ea-b16e-11eb-b464-005056bff430/210300%20France%20defense%20strategic-update%202021.pdf.

182 Ministère des Armées, 'Vision Stratégique Du Chef D'État-Major Des Armées' [Strategic Vision of the Chief of Defence Staff], October 2021, https://www.defense.gouv.fr/sites/default/files/ema/211022_EMACOM_VisionStrategiqueCEMA_FR_Vdef_HQ%20%282%29.pdf.

183 Ministère des Armées, 'Document de Référence de l'Orientation de l'Innovation de Défense' [Reference Document on Orientation, Innovation, and Defence], 2022, https://www.defense.gouv.fr/sites/default/files/aid/DrOID-2022.pdf.

184 Palais Elysée, 'National Strategic Review 2022', 2 December 2022, p. 47, http://www.sgdsn.gouv.fr/uploads/2022/12/rns-uk-20221202.pdf.

185 *Ibid*, p. 11.

186 Palais Elysée, 'Defence and National Security Strategic Review 2017', 15 October 2017, pp. 48 and 68, https://www.dsn.gob.es/sites/dsn/files/2017%20France%20Strategic%20Review.pdf.

187 See, for example' the priorities under Ministère des Armées, 'Document de Référence de l'Orientation de l'Innovation de Défense', https://www.defense.gouv.fr/sites/default/files/aid/DrOID-2022.pdf.

188 Ministère des Armées, 'INSTRUCTION N° 2067/ARM/CAB/CC6 relative à l'innovation de défense au sein du ministère des Armées', Cabinet de la Ministre, 7 May 2020, p. 3, https://www.defense.gouv.fr/sites/default/files/aid/IMID du 7 mai 2020.pdf.

189 Agence d'Innovation de Défense, 'Innovation de Défense: Bilan d'Activitiés 2021', 2021, p. 14, tps://www.defense.gouv.fr/sites/default/files/aid/Bilan%20d%27activités%202021.pdf.

190 *Ibid*.

191 Assemblée Nationale, 'Avis fait au nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de la Loi de Finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense par M. Fabien Gouttefarde, MP'.

192 Marc Watin-Augouard, 'The French "Digital Defence Agency" has been established', inCyber, 25 May 2021, https://incyber.org/en/the-french-digital-defence-agency-has-been-established/.

193 Stephanie Pezard, Michael Shurkin and David A. Ochmanek, 'A Strong Ally Stretched Thin: An Overview of France's Defense Capabilities from a Burdensharing Perspective', RAND Corporation, 2021, p. 30, https://www.rand.org/pubs/research_reports/RRA231-1.html.

194 Ministère des Armées, 'Vision Stratégique Du Chef D'État-Major Des Armées', p. 10.

195 Soare, 'Cooperative Edge: Key Drivers of Defence Innovation in Multinational Organisations like NATO and the EU'.

196 Jean-Pierre Devaux and Gaspard Schnitzler, 'Defence Innovation: New Models and Procurement Implications, The French Case', Armament Industry European Research Group, September 2020, p. 6, https://www.iris-france.org/wp-content/uploads/2020/09/63-Policy-Paper-Def-Innov-France-September-2020.pdf.

197 *Ibid*, pp. 9–10.

198 Sylvie Matelly, 'Defense Innovation and the Future of Transatlantic Strategic Superiority: A French Perspective', German Marshall Fund of the United States, 9 April 2018, https://www.gmfus.org/news/defense-innovation-and-future-transatlantic-strategic-superiority-french-perspective.

199 See Thierry Burkhard, 'French Army Chief: "Military Force is Making a Brutal Return to the International Scene"', *Le Monde*, 11 November 2022, https://www.lemonde.fr/en/opinion/article/2022/11/11/french-army-chief-military-force-is-making-a-brutal-return-to-the-international-scene_6003869_23.html; Davide Basso, 'France Not Ready for High-intensity War Says Former Army Chief', Euractiv, 9 November 2022, https://www.euractiv.com/section/politics/news/france-not-ready-for-high-intensity-war-says-former-army-chief/; and Cédric Pietralunga, 'French Military Chiefs Sound the Alarm on the State of the Armed Forces', *Le Monde*, 13 August 2022, https://www.lemonde.fr/en/international/article/2022/08/13/french-military-chiefs-of-staff-sound-the-alert-on-the-state-of-their-troops_5993519_4.html.

200 Assemblée Nationale, 'Avis Fait au Nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet

de la Loi de Finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense par M. Fabien Gouttefarde, MP'.

201 Preligens, 'Earthcube Overshoots Its Competitors', 22 September 2020, https://www.preligens.com/resources/press/earthcube-overshoots-its-competitors; and Pierre Tran, 'French Intelligence Agency Wants AI to Help Sort Masses of Raw Data', DefenseNews, 5 February 2018, https://www.defensenews.com/global/europe/2018/02/05/french-intelligence-agency-seeks-ai-to-support-analysts/.

202 European Defence Review, 'TALIOS Optronic Pod Qualified by French Defence Procurement Agency', EDR Magazine, 19 November 2018, https://www.edrmagazine.eu/talios-optronic-pod-qualified-by-french-defence-procurement-agency and MBDA Missile Systems, 'MBDA Collaboration Wins National Engineering Award for Work with Artificial Intelligence', 5 July 2019, https://www.mbda-systems.com/press-releases/le-programme-2aci-recoit-le-prix-aat-ingenieur-general-chanson/.

203 Thales, 'Thales and Dassault Aviation Win Contract for France's New Strategic Airborne Intelligence Programme', 14 January 2020, https://www.thalesgroup.com/en/worldwide-defence/radio-communications/news/thales-and-dassault-aviation-win-contract-frances-new; Thales, 'Collaborative Anti-Submarine Warfare', 2021, https://www.thalesgroup.com/en/markets/defence-and-security/naval-forces/underwater-warfare/collaborative-anti-submarine-warfare.

204 Maggie Gray and Amy Ertan, 'Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment. Appendix A – Country Profiles', NATO Cooperative Cyber Defence Cyber of Excellence, December 2021, pp. 16–18, https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_Appendix-A_A4.pdf.

205 Assemblée Nationale, 'Avis Fait au Nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de la Loi de Finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense par M. Fabien Gouttefarde, MP'.

206 Machi, 'France Approves Final Phase of Artemis Big-data Processing Platform' and Atos, 'ATHEA Selected by the French Ministry of the Armed Forces for Last Phase of Project ARTEMIS.IA', *GlobeNewswire*, 11 July 2022, https://www.globenewswire.com/en/news-release/2022/07/11/2477276/0/en/ATHEA-selected-by-the-French-Ministry-of-the-Armed-Forces-for-last-phase-of-project-ARTEMIS-IA.html.

207 French Land Army, 'Operational Superiority: A Battle-hardened Army Able to Commit in All Conflicts Up to a Major Confrontation', 2022, https://www.defense.gouv.fr/sites/default/files/terre/2022-Infographie-Vision-Strategique-anglaise.pdf.

208 Sopra Steria, 'Sopra Steria Chosen by the French Ministry of Defence to Implement Brasidas, the Single New Information System for Aerospace in Service Support', 25 March 2021, https://www.soprasteria.com/newsroom/press-releases/details/sopra-steria-chosen-by-the-french-ministry-of-defence-to-implement-brasidas-the-single-new-information-system-for-aerospace-in-service-support.

209 Assemblée Nationale, 'Avis Fait au Nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de la Loi de Finances pour 2022 (n° 4482), Tome II, Défense, Environnement et Prospective de la Politique de Défense par M. Fabien Gouttefarde, MP'.

210 Ministère des Armées, 'Projet de Loi de Finances 2023 - Loi de Programmation Militaire 2019-2025', p. 28.

211 Ursula von der Leyen, 'The Digital Transformation of the Bundeswehr', St. Gallen Business Review, 9 August 2018, https://www.stgallenbusinessreview.com/the-digital-transformation-of-the-bundeswehr/.

212 *Ibid*.

213 German Federal Government, 'Artificial Intelligence Strategy of the German Federal Government: 2020 Update', December 2020, https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf.

214 German Federal Government, 'Data Strategy of the Federal Government: An innovation strategy for social progress and sustainable growth', 27 January 2021, https://www.bundesregierung.de/breg-de/suche/data-strategy-of-the-federal-german-government-1950612.

215 Author interview with defence representative, September and December 2022.

216 Bundeswehr, 'Dritter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung' [Third Report on the Digital Transformation of the Federal Ministry of Defence], February 2021, p. 4, https://www.bmvg.de/resource/blob/5060250/6f695b7797b03986dd6eabf9946b5a38/download-3-digitalbericht-data.pdf.

217 *Ibid*.

218 Bundeswehr, 'Digitalisation in the Army', https://www.bundeswehr.de/en/organization/army/capabilities/digitalisation.

219 *Ibid*.

220 German Federal Government, 'Strategy Paper of the Federal Government on Strengthening the Security and Defence Industry', February 2020, p. 3, https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie-en.pdf?__blob=publicationFile&v=4.

221 Bundeswehr, 'Dritter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung' [Third Report on the Digital Transformation of the Federal Ministry of Defence], p. 37.

222 *Ibid*, p. 31.

223 Gray and Ertan, 'Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States Strategies and Deployment. Appendix A – Country Profiles', pp. 19–21, https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_Appendix-A_A4.pdf.

224 German Federal Ministry of Defence, 'Military Scientific Research Annual Report 2015: Defence Research for the German Armed Forces', 2015, https://www.bmvg.de/resource/blob/13614/49cb1a0b29c0d%2092521c7e2f59a3f6b6e/g-03-download-military-scientific-research-annual-report-2015-englisch-data.pdf.

225 Cyber Innovation Hub, 'Innovation projects', 2022, https://www.cyberinnovationhub.de/innovation/innovationsvorhaben.

226 German Federal Ministry of Defence, 'Defense budget 2021', December 2020, https://www.bmvg.de/de/themen/verteidigungshaushalt/verteidigungshaushalt-2021.

227 Systematic, 'C4I software for the digitalisation of the German Army', 10 March 2022, https://systematic.com/en-gb/industries/defence/news-knowledge/news/2022_c4i-across-the-german-armed-forces/.

228 Bundeswehr, 'Dritter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung' [Third Report on the Digital Transformation of the Federal Ministry of Defence], p. 39.

229 Bundeswehr, Zweiter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung' [Second Report on the Digital Transformation of the Federal Ministry of Defence], March 2020, pp. 19–23, https://www.bmvg.de/resource/blob/258260/cc60ba7e2570976df105baf97080fe45/20200312-download-zweiter-bericht-digitale-transformation-data.pdf.

230 Mölling and Schütz, 'Defence Innovation: New Models and Procurement Implications: The German Case', p. 9.

231 German Federal Ministry of Defence, 'Military Scientific Research Annual Report 2021**:** Defence Research for the German Armed Forces', 2022, https://www.bmvg.de/resource/blob/5536306/2b3d58bd18d845abe6b2e31d8caea4b6/military-scientific-research-annual-report-2021-data.pdf.

232 Soare and Pothier, 'Leading Edge: Key Drivers of Defence Innovation and the Future of Operational Advantage'.

233 Bastian Giegerich and Maximilian Terhalle, *The Responsibility to Defend: Rethinking Germany's Strategic Culture*, *Adelphi* 447 (Abingdon: Routledge for the IISS, 2021).

234 Giegerich and Schreer, 'Germany's New Defence Policy: The 100 Billion Euro Question'.

235 Mölling and Schütz, 'Defence Innovation: New Models and Procurement Implications: The German Case', p. 10.

236 German Federal Ministry of Defence, 'Information from the Parliamentary Commissioner for the Armed Forces Annual Report 2021 (63rd Report)', 15 March 2022, pp. 52–53, https://www.bundestag.de/resource/blob/901610/fc410cdd893ba69d52b8cb55ed1fb715/annual_report_2021_63rd_report-data.pdf.

Acknowledgements

The authors are grateful to all the governmental, industry and academic experts who generously donated their time and insights during various events and interviews organised to support this analysis. The authors are also grateful to Dr Bastian Giegerich and Dr Ben Schreer, who reviewed and provided comments on earlier versions of the report. The authors wish to thank Beryl Thomas and Fara Breuer for the research assistance provided during the project.

IISS

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GBcorp Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org