Policy Research on International Services and Manufacturing

New Technology and the Changing Military Industrial Complex

J Paul Dunne
PRISM, University of Cape Town, South Africa

Elisabeth Sköns
Stockholm International Peace Research Institute, Sweden

Working Paper Series
Number 2021-2

Acknowledgments

We are grateful to Ron Smith, Lucie Béraud-Sudreau, Michael Brzoska, Vincent Boulanin, Paul Holden, Christos Kollias, Nick Lawrence, Nan Tian and Herbert Wulf, for comments, but the usual disclaimer applies.

Recommended citation:

Dunne, J. P., and Sköns, E. 2021. "New Technology and the Changing Military Industrial Complex". *PRISM Working Paper 2021-2.* Cape Town: Policy Research on International Services and Manufacturing, University of Cape Town.

New Technology and the Changing Military Industrial Complex

Dunne, J. Paul and Sköns, Elisabeth

PRISM Working Paper Number 2021-2
University of Cape Town

Abstract

This paper considers what could be a fundamental development in the defence industrial base (DIB), namely the increased involvement of commercial technology companies in military-related business. It focusses on developments in the US, recognizing that these are often the precursors of change in the international arms industry. After an outline of the dynamics and longer-term post-Cold War developments in the international arms industry, it investigates recent changes in the Pentagon's attitudes and policies to gain access to new technologies from the commercial and academic sectors. It also considers the military, technological and political drivers that have led to these technologies being sought from commercial companies for military use. It then considers the recent engagement of the major commercial technology companies in activities for the military sector and what is driving them to take up military contracts. The review is based on open source information as available in official government reports and data, conference reports, academic literature, and specialist and ordinary news items. Finally, it considers what these developments imply for the dynamics of the arms industry and the relationships within the DIB and the military industrial complex (MIC).

Keywords: New technology; defence; security; software; IT; DIB; MIC; cloud

POLICY RESEARCH ON INTERNATIONAL SERVICES AND MARKETING

Policy Research in International Services and Manufacturing (PRISM) is a research and policy unit located within the School of Economics. PRISM provides a lens to focus research and policy work broadly on issues of globalization, trade and industrialization. It is home to a number of related research activities, projects and programmes concerned with issues of globalization, global value chains, industrialization paths, international trade, foreign investment, the defence industry, policy governance, infrastructure development, the role of knowledge intensive services, innovation, and international competitiveness. Another feature of PRISM's work has been its applied focus, responding to economic policy questions issues in South Africa, the rest of Africa and beyond

School of Economics Building, Middle Campus, University of Cape Town Private Bag, Rondebosch 7701, Cape Town, South Africa
Tel: +27 (0)21 650 4470
Web: www.prism.uct.ac.za

1. Introduction

Since the mid-2010s, there have been developments in defence policy that have aimed to increase the engagement of commercial technology companies in military-related activities. This represents a significant change in procurement policy and could have a significant impact on the arms industry, an industry that has already seen considerable change, with the end of the Cold War and changes in the international security environment. It also potentially has profound implications for the relationship between the arms industry, the government and the military.

The first shock to the industry came when world military expenditures began to fall in the late 1980s and continued on a downward trend during the first post-Cold War decade. At the same time, the fixed costs of R&D for major systems continued to grow, both for platforms and for the infrastructure (e.g. satellites, strategic air assets) and the information-based systems needed to support network-centred warfare (Dunne and Sköns, 2010). Changes in technology, with increasing importance of electronics and of information and communications technology (ICT) in military technology, resulted in an increased need for enabling technology in weapon systems. This led to a major restructuring of the arms industry and in the relations between it, the government and the military. Arms contractors changed, becoming systems integrators, outsourcing nationally and internationally, spinning in civil technologies and components, rather than spinning off innovations for the civil sector. These processes resulted in a reduced number of dominating companies but of much larger size, and increased reliance on foreign components. However, the traditional defence producers, specializing on the military market remained dominant, partly through takeovers to acquire expertise in new areas. There is little evidence to suggest that the links between the industry, the military, government and the legislature weakened. Rather, it would still seem that it is a political rather than economic logic that controls the international arms market. There has been change, but also a remarkable degree of continuity. (Dunne and Sköns, 2010).

Recent developments have the potential to have even more significant effects on the arms industry and its relations with the government and the military, although at present their impact is little understood. Most visible and striking is the ongoing process in the US Department of Defense (DoD) to award a contract potentially worth $10 billion for a cloud infrastructure system, called Joint Enterprise Defense Infrastructure (JEDI). This contract, which is considered one of Pentagon's most high-profile technology contracts in years is running over 10 years. It aims to build a system to store, process and link together a vast amount of data at all classification levels into a single, unified architecture, allowing the US military to improve communication with soldiers on the battlefield and use artificial intelligence (AI) to speed up its war planning and fighting capabilities.[1] The decision in October 2019 to award the contract to one of the Big Five US commercial technology companies,[2] Microsoft, provoked a legal protest from one of the other Big Five, Amazon, who was the main remaining competitor and the expected winner of the contract award.[3] The legal protest from Amazon, referring to flaws in the evaluation process, forced the DoD to

[1] 'One year in the Pentagon's push for a revolutionary cloud: A look at key moments in one of the Pentagon's most important tech procurements', Nextgov.com, Aug. 2018, https://www.nextgov.com/feature/jedi-contract/ .
[2] The Big Five US tech companies are Amazon, Apple, Facebook, Google (Alphabet) and Microsoft.
[3] 'Microsoft Wins Pentagon's $10 Billion JEDI Contract, Thwarting Amazon', NYT Online, 25 Oct. 2019, https://www.nytimes.com/2019/10/25/technology/DoD-jedi-contract.html ; 'Microsoft Wins Pentagon Deal Over Amazon, NYT, 26 Oct, 2019, Section A, Page 1; and 'Pentagon awards $10-billion 'war cloud' deal to Microsoft, snubs Amazon', Deutsche Welle, 26 Oct. 2019.

make a re-evaluation of the bidding process.[4] After several extensions over a period of 10 months, this resulted in the announcement on 4 September 2020 of the decision to award the contract again to Microsoft - with Amazon declaring it would continue to protest.[5] By March 2021, the legal issues were still not resolved[6].

This case of a competition between big commercial technology companies for a major military contract with direct warfighting implications raises the question of whether the arms industry is undergoing another phase of change and if so, what this change involves for the arms industry, for the broader defence industrial base (DIB) and for the military industrial complex (MIC). The DIB refers to the overall national resources required for providing and maintaining the national requirements of military equipment, in terms of R&D, production and maintenance. The MIC refers to the coalition of actors with vested interests in the military sector, thus widening the perspective to encompass also the dynamic of economic, political and social factors influencing the DIB. Such coalitions of vested interests could include members of the armed forces, of the civilian defence bureaucracy, of the legislature, and of the arms industry and arms industry workers. Whether these actors have common or conflicting interests, their competition for resources tends to generate internal pressures for military spending. Interestingly, the origin of the term MIC as well as the acknowledgement of its existence is President Eisenhower, a Republican and ex-military man. In his 1961 end-of-term address to the nation, he drew attention to 'the total influence—economic, political, even spiritual—'created by the 'conjunction of an immense military establishment and a large arms industry', which the US had been compelled to create during the World War II. He urged the US government and citizenry to 'guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. [7]

This paper considers the changes that have been taking place and what they might mean for the future, focusing on developments in the US, recognizing that these are often the precursors of change in the international arms industry and that most of the major commercial technology companies are also American. Specifically, it raises the question of whether recent developments in defence policy and arms acquisitions, as exemplified by the JEDI, mean that the arms industry is undergoing another phase of structural and relational change. Section 2, provides background and context, outlining the main characteristics of the DIB and MIC focusing on post-Cold War developments. Section 3 then considers the changing approaches to military technology and the arms procurement system and the drivers behind these changes. Section 4 considers some of the new technology projects with commercial technology company engagement in more detail and some of the internal reactions within the tech companies. Section 5 considers the new roles of the commercial technology industry in the military sector,

[4] In fact it was preceded by earlier legal protests, including from another big technology company, Oracle, after both Oracle and IBM had been losing out from the competition process in April 2019, as well as by a decision by a third Big Five company, Google, to pull out of participation in the competition for the contract, referring to possible conflict with its corporate values. 'Google drops out of Pentagon's $10 billion cloud competition', Bloomberg.com, 8 Oct. 2018, https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition ; and 'Google drops out of competition for a $10 billion defense contract because it could conflict with its corporate values', Businessinsider.com, 9 Oct. 2018, https://www.businessinsider.com/google-drops-out-of-10-billion-jedi-contract-bid-2018-10?r=US&IR=T.

[5] 'Pentagon awards JEDI cloud contract to Microsoft for the second time, NextGov, 4 Sep. 2020, https://www.nextgov.com/it-modernization/2020/09/pentagon-awards-jedi-cloud-contract-microsoft-second-time/168259/

[6] https://www.bloomberg.com/news/articles/2021-03-05/microsoft-s-10-billion-pentagon-deal-at-risk-amid-amazon-fight

[7] Dwight D. Eisenhower, 'Farewell Address', in Albertson, D. et al., *Eisenhower as President* (American Century Series, Hill and Wang. New York, 1963), p. 162.

the possible responses of the traditional defence contractors and the implications for the nature of the DIB and the MIC. Finally, section 6 provides a summary and some conclusions on what these developments imply for the arms industry and the relationship within the DIB and the MIC in the US and for the international arms industry.

2. Development of the DIB/MIC

During the Cold War, the defence industry took on a particular structure that continues to influence developments now. The national government was the main customer and regulated exports and determined its size and structure. This monopsonistic structure of the market led to an emphasis on performance rather than cost of the products (high-technology military systems). Risk was borne by government, which often financed R&D and, in some cases, provided investment in capital and infrastructure. Elaborate rules and regulations on contracts, were developed to compensate for the absence of any form of competitive market and to assure public accountability. This all meant that close relations developed between contractors, the procurement executive and the military, notably what is termed the 'revolving door' in which military and civil servants move to defence contractors they had dealings with and staff from defence contractors move into the bureaucracy.

These characteristics tended to favour those firms who specialise in defence work, as they knew their way around the red tape, had useful contacts and became experts at negotiating contracts with government. These were different skills to those needed in commercial markets. Firms used strategies such as 'buy ins', where they understated the risk or cost to win initial contracts, with a view to making up the losses later, with the inevitable changes that allowed renegotiation of contracts or additional payments. Defence companies became experts at getting contracts out of government and these skills and the structure of the market meant that there were both barriers to entry and barriers to exit. This led to the Cold War DIB showing remarkable stability in terms of its composition of main contractors. Monopsony in the defence market also helped to create near-monopolies for certain companies particularly in smaller countries. Outside of the US, there was a prevalence of companies that were national monopolies or close to it. Any competition was going to come from foreign firms, but governments tended to protect national companies, wishing to maintain a national DIB. Much of the work on the MIC sees a negative impact of vested interests as a fairly clear and constant feature of the Cold War. The argument is that in the absence of a 'hot war' between the two superpowers to test the strength of the adversary, it was possible to overemphasize and exaggerate threats. These developments then justified high levels of military spending and allowed inefficiencies to develop (Dunne and Sköns, 2010).

World military spending peaked in the late 1980s, then declined by roughly one-third during the subsequent decade, first as a result of improving East-West relations and then with the end of the Cold War. The international arms trade dropped by a half between the 1982 all-time high and the 1995 trough, then fluctuated somewhat until it began to increase consistently in 2003 (The SIPRI Arms Transfers Database). These changes had a direct impact on the demand for the products of the MIC and the environment in which they operated, calling into question the ability of even the major countries to maintain a comprehensive domestic defence industrial base. Governments found it harder to justify previous levels of support for the industry and 'competitive procurement policies aimed at value for money were introduced in a number of countries' (Dunne and Sköns, 2010).

In 1999 the trend reversed and in 2001 it turned into a strong growth, particularly in the US, due to the massive spending made possible under the 'global war on terror' label justified primarily with the war in Afghanistan[8]. Linked to the war on terrorism, there was also an explicit shift from a threat-based strategy to a capability-based strategy. While giving primacy to the development of transformative technologies and strategies, it retained a two-theatre war requirement and the 'legacy' weapon programmes, as articulated in the 2001 US Quadrennial Defense Review (Gold, 2002). Allowing for both continued investment in legacy systems and a transformation of military affairs, this shift in strategy allowed for the massive increase in US military spending during the first decade of the new millennium[9].

The wars in Afghanistan and Iraq were funded through supplemental appropriations outside the regular annual defence budget requests, according to which all war-related appropriations (i.e. used specifically for the war) were not subject to standard legislative oversight. This practice had two important implications: it produced an overly optimistic picture of the funding requirement for the war and it reduced the level of legislative oversight. In 2006, new DoD guidance for war appropriation requests made it possible for the armed services to include virtually anything in their requests for war-related appropriations. This provided scope for adding on non-war related items in a rapidly expanding defence budget (Perlo-Freeman, 2010). This practice has continued for military activities in Syria and elsewhere. US funding of war-related and international emergency activities through supplementary appropriations during the budget years FY2001-2019 amounted to a total of $2 trillion, of which $1.835 trillion was for the DoD.[10]

In addition to the changes in the level of demand for arms, new technologies enabled new types of warfare and changed the nature of demand. Communication and control technologies became increasingly important in the theatre of military operations. Network-centred warfare, the use of satellites, communications equipment and multi-node networks changed the nature of demand. This was part of the Revolution in Military Affairs (RMA), a term used to emphasise the way that improvements in information technology, precision targeting and smart munitions created the possibility of a new form of warfare, network-centred warfare. It also changed the nature of military technology, with increased importance of software and ICT and an increase in their share of costs in the production of weapons systems. The internet came to play an important role in the development of communications, but it also provided a further area of potential security threats. Uncertainty about the enemy and the growth of 'homeland security' added new types of demand, making communications and surveillance technologies increasingly important (Boulanin 2013; Smith 2009)[11]. In addition, the growth of peacekeeping

[8] As well as the war in Iraq, although this war was based primarily on US assertions of Iraqi non-compliance with its international obligations regarding weapons of mass destruction.

[9] The Quadrennial Defense Review 2001, which was released less than 3 weeks after 9/11. It articulated a shift in US military strategy. "Instead of basing force structure on the ability to meet specific and explicit threats, the focus would be on developing forces with a range of capabilities to meet both unforeseen and predictable threats." (Gold (2002) This change represented a strengthening of several existing trends, including 1) the expanding use of IT in RMA, 2) the development of defences against asymmetric threats and 3) the renewed attention to homeland defence. It also provided both for continued procurement of legacy systems and budgetary resources for the development, introduction and deployment of transformative technologies and strategies to maintain US military supremacy. Thus, it paved the way for massive increases in US military spending.

[10] McGarry, B.W. and Morgenstern, E.M., *Overseas Contingency Operations Funding: Background and Status*, CRS Report R44519, US Congressional Research Service, Washington DC, 6 Sep. 2019, accessible at https://crsreports.congress.gov/search/#/?termsToSearch=R44519&orderBy=Relevance

[11] Some security theorists have identified these developments as different waves of RMAs (Raska, 2020).

roles around the world, created somewhat different military systems and personnel requirements (Dunne et al 2006).

These changes in the level and composition of demand led to a number of important developments on the supply side, including increased concentration, technological change, subcontracting and internationalisation. The end of the Cold War did not bring about the expected diversification of the defence industry to civil products. Instead there was a rapid process of ownership concentration through mergers and acquisitions.[12] The increased fixed costs in production that assisted industrial restructuring also led to arms producers resorting to commercially available civilian technologies and products, a marked change from the pre-eminence of military technology up to the 1990's (Smith, 2009). Many areas of technology which were once the preserve of the military and security services, such as cryptography, became dominated by commercial applications and increased numbers of civil components and sub systems went into major weapon systems. For example, semiconductors became increasingly used in fighter planes, such as the Eurofighter and F35 and cruise missiles.[13] Subcontracting became increasingly important, increasing links with the civil sector and bringing new types of company, particularly from the electronics and IT sectors, into the defence industrial base (Dunne et. al., 2007a, b).

Another important factor was the internationalisation of arms production in the post-Cold War period. This has taken two forms, the internationalisation of ownership and the internationalisation of supply chains. High costs of high-technology research and development combined with smaller national production runs led to international collaboration and industrial restructuring, with considerable internationalization of the content of advanced weapons systems (Dunne, 2006a). International supply chains provided flexibility and potential cost reductions for firms, reducing their in-house production, but dependence on international subcontractors became a concern, particularly for the US. Indeed, in the US, this concern over the growing use of foreign components in weapons systems led to the Defence Production Act of 1950 being used on a number of occasions to require domestic producers to have the capability to produce those components[14].

DoD showed a commitment to cybersecurity, to secure its networks and to engage in cyber warfare and protection, in its FY2012 budget proposal, by committing to planned spending of $2.3 billion. The response of the larger defence contractors was to buy up smaller cybersecurity and intelligence services companies.[15] Indeed, the Washington Post suggested

[12] In 1993 a merger wave was stimulated by the 'last supper' when Defense Secretary William Perry, told a dinner of defence industry executives that they were expected to start merging (Pages, 1999: 212-213). In 1997, the merger policy was reversed, since it had become evident that it did not produce the anticipated savings for the DoD (Sköns 2010: 238). However, the mega-merger trend continued. In 2002, the US DOD reported that the US arms industry was in a late stage of consolidation after having merged what was 51 separate defence business units in 1980 into 4 large defence companies in 2001. The last mega-merger was the takeover of aerospace and information technology company TRW by Northrop Grumman in 2002 (Sköns and Baumann, 2003: 381).

[13] Semiconductors have also become a major part of the technological rivalry with China https://foreignpolicy.com/2020/10/23/semiconductors-china-united-states-defense-dependency/

[14] Indeed, as early as 1985 the Congressional Defence Joint Oversight Committee on Foreign Dependency, found that the guidance system of an air to air missile had 16 foreign produced parts. Legislation was used to require domestic producers to have the capability to produce the components. General weakness of defence industrial capacity discussed in https://www.defensenews.com/pentagon/2019/06/27/here-are-the-biggest-weaknesses-in-americas-defense-sector/

[15] For example, BAE Systems acquired Norkom Group ($344m), Detica ($1b.), ETI A/S ($212m) and stratsec.net ($23m); Raytheon acquired Applied Signal technology ($490m); and Boeing acquired Argon ST

that the large arms producers were driving overall mergers and acquisition activity.[16] By FY2021, the US budget request for cybersecurity amounted to $9.8 billion for DoD's unclassified cybersecurity efforts within an overall total for the federal government of $18.8 billion.[17]

In 2014 Reuters reported that the Pentagon repeatedly waived laws banning Chinese-built components on U.S. weapons in order to keep the $392 billion Lockheed Martin F-35 fighter program on track in 2012 and 2013, even as U.S. officials were voicing concern about China's espionage and military build-up.[18] This led to an amendment to the National Defense Authorization Act for Fiscal Year 2012 which was adopted in the Senate and signed by President Obama. From then on, the administration increasingly showed concern about losing the lead on Russia and China in weapons technology.

With the Trump administration there was a push for arms exports from 2018, but also a hardening of attitudes towards China, as reflected in the 2018 National Defense Strategy. Pressure was put on companies to reduce technological dependence on Huawei and prevent the export of technology to them. Huawei were also banned from 5G telecom systems and pressure was put on other countries to do the same.[19] Such anti-Chinese actions by the Trump administration created international tensions and problems for the tech sector in the US, as the US has no firms with 5G capability and risks falling behind technologically. There have been suggestions of the US approaching Ericsson, who along with Nokia, is the only European firm with 5G capability and a potential supplier of the technology.[20] The US attorney general William Barr suggested that the US should consider 'aligning itself with Nokia and/or Ericsson through American ownership of a controlling stake, either directly or through a consortium of private American and allied companies'.[21] This was subsequently clarified by a White House spokesperson as meaning a partnership with the telecom industry, which, he said, is something entirely different than buying shares with taxpayers' money. [22]

Another major development that introduced some new faces was the significant expansion of the military services industry from the end of the Cold War. This resulted from the outsourcing of functions that once were provided by military forces or defence ministries to private

---

($775m) in 2010. 'Defense industry increases cybersecurity acquisitions', Clearancejobs, 28 Jun 2011. https://news.clearancejobs.com/2011/06/28/defense-industry-increases-cybersecurity-acquisitions/ . See also, SIPRI YB 2011. Boulanin, V., Major arms industry acquisitions, 2010', in SIPRI Yearbook 2011, OUP, Oxford, 2011, appendix 5B, pp 263-264.

[16] 'Defense contractors on the offensive', Washington Post, 26 Sep. 2010

[17] 'Federal Tech Guide to Trump's 2021 budget', NextGov, 10 Feb. 2020, https://www.nextgov.com/cio-briefing/2020/02/federal-tech-guide-trumps-2021-budget/163016/.

[18] https://ca.news.yahoo.com/exclusive-u-waived-laws-keep-f-35-track-204531422--sector.html

[19] https://uk.reuters.com/article/uk-usa-trump-arms-insight/arming-the-world-inside-trumps-buy-american-drive-to-expand-weapons-exports-idUKKBN1HO2Q2
https://www.economist.com/briefing/2020/07/16/americas-war-on-huawei-nears-its-endgame

[20] 'Pentagon vill knyta Sverige närmare' ['*Pentagon wants to tie Sweden closer'*], Dagens Nyheter, 13 Jan. 2019, https://www.dn.se/nyheter/sverige/pentagon-vill-knyta-sverige-narmare/; and 'Trump pratade Ericsson med Löfven', ['Trump talked Ericsson with Löfven'], *Dagens Industri*, published 15 Sep. 2019, updated 7 Feb 2020, https://www.di.se/ledare/ur-arkivet-trump-pratade-ericsson-med-lofven/ .

[21] 'Really? Is the White House proposing to buy Ericsson or Nokia?', New York Times, 7 Feb. 2020, https://www.nytimes.com/2020/02/07/business/dealbook/bill-barr-huawei-nokia-ericsson.html ; 'William Barr: USA bör överväga att köpa Ericsson' ['William Barr: USA should consider buying Ericsson'], Ny *Teknik*, 7 Feb. 2020, https://www.nyteknik.se/digitalisering/william-barr-usa-bor-overvaga-att-kopa-ericsson-6986687

[22] 'Inga amerikanska skattepengar till köp av Ericssonaktier' [*No American tax money for purchase of Ericsson shares], Ny Teknik*, 14 Feb 2020, https://www.nyteknik.se/digitalisering/inga-amerikanska-skattepengar-till-kop-av-ericssonaktier-6987649 .

companies and was expanded greatly during the war in Iraq (Singer 2003; Wulf 2005). This led to a significant change in both the structure of the DIB, with new companies, such as KBR, previously owned by Halliburton, becoming a major DoD contractor for its provision of construction in conflict zones (Briody, 2004) and in the nature of the MIC, as companies providing military services are often engaged directly in conflict zones. Their interests are different and more problematic than the vested interests of military goods-producing companies, whose products are also in high demand during peacetime (Perlo-Freeman and Sköns 2008, 13).

These developments all led to a defence industrial base that was looking rather different to the one inherited from the Cold War. In the US it was still dominated by a few main contractors that had merged and made acquisitions to retain their position. In other countries there were limited cross country mergers, but there was some restructuring and companies that survived remained dependent on national governments and their support for arms exports. There was change but also continuity, as Dunne et al (2020) argue.

Since the mid-2010s, there have been further developments taking place in the US that have the potential to engender more profound changes in the structure of the defence industrial base, with implications for the international arms industry. Specifically, an important change in approaches to military technology starting in the 2010s, the deployment of some major high technology contracts to develop information technology and cyber security for the military sector and the engagement of major civil tech companies. The new Biden administration has, in 2021, has supported plans for the military deployment and use of new and emerging technologies. There will be federal funding for such technologies within a strongly collaborative structure between government agencies, commercial companies and universities. These changes, and the ethical issues raised for the companies, are discussed in the next two sections.

3. Changing DoD approaches to military technology

In the early 2010s, efforts began within the US DoD to develop a strategy to sustain and advance US global military-technical superiority through an increased emphasis on technological innovation rather than relying on continued expansion of conventional forces. This took place in a situation in which strong cuts in US military spending were foreseen after a decade (2001-2010) of strong increases in US military spending driven by the wars in Afghanistan and Iraq. The foreseen cuts in military spending were due partly to the successive withdrawal of US troops from Iraq since 2007, but primarily to financial constraints caused by a soaring federal government budget deficit following the 2009 global economic and financial crisis. In July 2011, Congress agreed on a Budget Control Act, which imposed ceilings on government spending over the next 10-year period (2012-2021), including for defence, and subsequently automatic spending cuts (sequestration) over the same period, equally split between military and non-military spending (Sköns and Perlo-Freeman, 2012:162-166).

Against the background of a government spending crisis and the ending of the wars in Afghanistan and Iraq, which necessitated a reshaping of the armed forces, a review of US national security and defence strategy was commissioned. The Defense Strategic Guidance, presented in January 2012 to guide military priorities and spending over the next decade (2012-2021), identified a number of primary missions that required increased spending. These were counterterrorism and irregular warfare; deterrence and defence; power projection capabilities

in the face of asymmetric capabilities; and advanced and effective operational capabilities in cyberspace and space. In contrast, it included cuts for conventional ground forces and for some major systems designed for the cold war, the so-called 'legacy' systems.[23] In this environment of financial constraints and wartime transition, in November 2014, the DoD presented a Defense Innovation Initiative to 'establish a broad department-wide initiative to pursue innovative ways to sustain and advance our military superiority for the 21st century'. [24] The main element of this initiative was to 'identify a third offset strategy that 'puts the competitive advantage firmly in the hands of American power projection over the coming decades.' [25]

The third offset strategy followed on from the second offset strategy in the 1970s, which was considered to have lain the foundation for the network-centric warfare and precision strikes that had enabled US military supremacy post-Cold War. The first offset strategy in the 1950s had enabled the use of tactical nuclear weapons to offset the Soviet numerical advantage in conventional force. [26] Each of these strategies had been based on a specific technology. The first offset strategy was based on the miniaturization of nuclear components, while the second strategy was based on the development of digital, information technologies, new sensors and stealth, which enabled the development of precision-guided weapons. The objective of the third offset strategy was to develop and apply emerging and disruptive technologies in innovative ways to offset the potential future military technological advantage of adversaries and so sustain US military supremacy into the 2030s. However, while the previous offset strategies had clear visions about the types of weapons systems and technologies that the strategies were aiming at, the third strategy was more open-ended, aside from a general focus on artificial intelligence and autonomy in weapon systems (Boulanin and Verbruggen, 2017). It was clear early on that this required going beyond the traditional arms suppliers and needed a major effort to access commercially developed technologies.[27]

Ashton Carter, who began his term as Secretary of Defense in February 2015, was instrumental in developing this new policy.[28] In April 2015, he made a speech at Stanford University, calling for a renewal and strengthening of the partnership between Silicon Valley and the DoD. He emphasized that for this to happen, the DoD would need to change, to become more open and to think outside the box, the implication being that otherwise civil technology companies

[23] US Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense,* DOD: Washington, DC, Jan. 2012.
[24] US Department of Defense, 'The Defense Innovation Initiative', Memorandum of the Secretary of Defense, Pentagon, Wash. DC, 15 Nov. 2014, <OSD013411-14 pdf.
[25] US Department of Defense, 'The Defense Innovation Initiative', Memorandum of the Secretary of Defense, Pentagon, Wash. DC, 15 Nov. 2014, <OSD013411-14 pdf>.
[26] Ellman, J. et al, *Defense acquisition trends 2015: Acquisition in the era of budgetary restraint*, CSIS, Wash DC, 2016.
[27] See the website of the Defense Innovation Initiative; *Defense Innovation Marketplace: Connecting Industry and the Department of Defense*, ttps://defenseinnovationmarketplace.dtic.mil/innovation/dii/
[28] Much of the thinking behind the policy can be attributed to Bob Work, US Deputy Secretary of Defense (2014-2017), subsequently engaged at the Center for New American Security (CNAS), 'Deputy Secretary: Third Offset Strategy bolsters America's military deterrence', *DoD News*, 31 Oct. 2016, https://www.defense.gov/Explore/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/; and 'Remarks by Deputy Secretary Work in Third Offset Strategy', US DoD, Newsroom, 28 Apr. 2016, https://www.defense.gov/Newsroom/Speeches/Speech/Article/753482/remarks-by-d%20eputy-secretary-work-on-third-offset-strategy/

wouldn't want to deal with DoD because of its procurement practices.[29] To facilitate cooperation, he initiated a series of changes at the DoD. First, personnel reforms to make it easier for DoD to bring the needed expertise. Second, the development of schemes to protect the intellectual property rights of the commercial partners. Third, the establishment of a new DoD organization in Silicon Valley, called the Defense Innovation Unit Experimental, DIUx, to serve as the hub for the DoD's 'communication with, knowledge of, and access to innovating, leading edge technologies from the tech startups and entrepreneurs'.[30] These changes represented a clear recognition that there were high barriers to entry, particularly because of the long timelines inherent in the federal acquisitions system, and that a cultural change was needed.[31] After a slow take-off of DIUx, Carter initiated a major overhaul of the organization in Spring 2016, bringing in a new leadership, opening a second office in Boston and making the unit report directly to him. The new leadership consisted of people with both military or DoD experience and Silicon Valley success, for example, Isaac Taylor, the founding head of operations at the Google[X] lab, the experimental group behind Google's self-driving cars.[32]

In 2016, DIUx launched the Commercial Solutions Opening (CSO) process to open up and streamline the arms procurement system for innovative commercial technologies. This was to allow the DIUx 'to prototype and acquire technology quickly, providing a streamlined and flexible process that makes it easier for commercial companies to do business with the Department of Defense.' Barriers to entry were reduced and companies only needed to submit short solution briefs to compete, rather than go through the usual procedures. The CSO process is seen as a major step towards DIU's goal to build a national security innovation base (NISB) 'to capture the best the commercial sector, industry, academia, and national labs have to offer.'[33]

The defense innovation strategy was based on the idea of involving academia and commercial technology industry in the transformation of military technology. One element for achieving this early on in the process was the Defense Innovation Board, which was set up in 2016 to provide the DoD with independent advice and recommendations, with its members recruited specifically for their expertise outside DoD. Since its establishment it has been chaired by Eric Schmidt, technical advisor at Alphabet (2017- present) and former CEO of Google and executive chairman of Google and its parent Alphabet (2001-2017). Other members from the civil tech companies include the vice president of Global Partnerships, Facebook, the vice president of Wireless Services, Google, and the co-founder and chairman of LinkedIn, Microsoft.[34] The involvement of leading commercial company figures in DoD advisory roles

[29] Carter, Ashton, 'Rewiring the Pentagon: Charting a new path on innovation and cybersecurity', Drell Lecture at Stanford University, Palo Alto, 23 Apr., 2015, US DoD Archives, Secretary of Defense Speech, https://archive.defense.gov/speeches/speech.aspx?SpeechID=1935

[30] For a detailed account of the purpose, challenges and tasks of the Defense Innovation Unit, see Hummel, R.H. and Schiller, K., 'Department of Defense's Innovation Experiment', Featured articles, Potomac Institute, 30 June 2016, https://www.potomacinstitute.org/steps/featured-articles/83-department-of-defense-s-innovation-experiment

[31] Defense Innovation Unit Experimental, *DIUx Commercial Solutions Opening: How to Guide,* www.diux.mil, 30 Nov. 2016.

[32] 'Pentagon shakes up Silicon Valley outreach', DefenseOne, 11 May 2016, https://www.defenseone.com/technology/2016/05/pentagon-shakes-silicon-valley-outreach/128198/; 'Carter announces version 2.0 of Defense Innovation Unit', https://www.defense.gov/Explore/News/Article/Article/757147/carter-announces-version-20-of-defense-innovation-unit-experimental/

[33] Defense Innovation Unit, Annual Report 2018, p1.

[34] 'Meet the Board', Website of the Defense Innovation Board, accessed 5 Sep. 2020. https://innovation.defense.gov/Members/ Amazon bought LinkedIn in 2016.

was an opportunity not only for the DoD to obtain advice and recommendations from technical experts, but also for the tech companies to promote their technologies and services.
There are a number of stories about these interactions. For example, during the course of 2016, the members of the DIB undertook a series of visits to Pentagon operations across the world to get an idea of their challenges. This was an opportunity also for assessing the military technology market. For example, a year after Schmidt, then CEO of Google, visited a drone-operations centre at Creech Air Force Base in Nevada, and witnessed the limited technology used, which meant that almost all reviewing of information was by humans, while recognition software was already widely available. Google won a $17 million subcontract to provide image recognition software to identify drone targets. [35] Such tours reflected and influenced the major change in government attitudes to new technologies that had been taking place.

With the incoming Trump Administration in January 2017, there was a return to major investments in conventional and nuclear weapons and a resumption of growing military expenditure from 2018 onwards, supported by the 2017 National Security Strategy, which identified China and Russia as US rivals, challenging the power, influence and interests of the USA.[36] Thus, after an 8-year period of falling US military spending (2010-2017), the military budget increased from $610 to $700 billion between fiscal years 2017 and 2018 – in spite of the still valid Budget Control Act of 2011 (Tian, et al. 2018: 158-160). The importance attached to advanced technologies for future warfare remained, but now within the new defense and security strategies and paired with a renewed strong emphasis on major traditional weapon systems. While there was little talk of the third offset strategy, it would seem the spirit remained. The 2018 National Defense Strategy recognized the need to develop DoD policies to guarantee US technological advantage and charged the DoD and Congress to build a national security innovation base (NISB) that included both traditional and non-traditional defense partners (US DoD, 2018).

In 2018, DIUx was made permanent and renamed DIU. It had expanded significantly, both in terms of size and authority. In its annual report for 2018, it reported how its mission had grown from its original focus of reinvigorating DoD outreach to commercial innovators to now sit 'at the nexus of commercial technology and national security in an era of resurgent great power competition and rapid, global diffusion of technological advancement'.[37] The procedures and engagement in defence contracting for making it easier for commercial companies delivering national security solutions are described on the DIU homepage. [38] The mission of DIU is three-fold: to accelerate DoD adoption of commercial technology; to transform military capacity and capabilities; and to strengthen the national security and innovation base. Its work focuses on five areas of technology where leading-edge capabilities are essential to 21st century military-

[35] 'How Amazon and Silicon Valley seduced the Pentagon', Propublica.org, 22 Aug 2019. https://www.propublica.org/article/how-amazon-and-silicon-valley-seduced-the-pentagon
[36] White House, *National Security Strategy of the United States of America*, White House, Wash. DC, Dec. 2017.
[37] Defense Innovation Unit, Annual Report 2018.
[38] "DIU has lowered barriers to entry into the defense market for commercial companies driving innovation in emerging and foundational technology areas. Our fast and flexible contracting process and commitment to establishing a clear path to path to large-volume defense contracts has created a new way for businesses work with the DoD on commercial terms at commercial speeds. Our team works with our Department partners and companies every step of the way. We help our DoD partners translate national security challenges into problem statements that draw in the best potential commercial solutions and guide the companies we work with through the process to a defense contract award. From the first time a potential customer reaches out to us with a challenge to the moment a new technology is fielded, the DIU team is there to facilitate easy collaboration between our DoD partners and vendors and execute prototype projects with speed and agility." US DoD, Defense Innovation Unit, https://www.diu.mil/solutions

technical advantage and are dominated by the commercial sector, namely artificial intelligence, autonomy, cyber, human systems, and space.[39] In November 2018, DIU received full contract authority, being granted authority to award so-called Other Transaction (OT) agreements, 'allowing it to set up internal contracting capabilities.'[40] Before then, the DIU had awarded all contracts through third party contracting offices within the DoD. The DIU was now an important player within the MIC.

Another DoD unit, The Joint Artificial Intelligence Center (JAIC), was set up in June 2018 to accelerate delivery of AI-enabled capabilities and the adoption of new artificial intelligence technologies developed in the commercial sector 'for the benefit of America's national security.'[41] Its standing was ratcheted up in February 2019 when the White House released an executive order on 'Maintaining American Leadership in Artificial Intelligence' and the DoD released a summary of an Artificial Intelligence Strategy, with JAIC as the focal point (US DoD 2018b).[42] To achieve its mission, to accelerate the delivery and adoption of AI, the JAIC has five areas of activities: Joint warfighting operations; 'warfighter health'; 'business process transformation'; 'threat reduction & protection'; 'joint logistics'; and 'joint information warfare (formerly cyber)'.[43] The strategy also emphasized the need for collaboration with academia and non-traditional centres of innovation in the commercial sector. By June 2020, the JAIC had a staff of 185 people, its budget had increased to $268 million in FY 2020 and the DoD budget for AI and machine-learning-related R&D had increased from $1.3 billion in FY2019 to $4 billion in FY2020.[44] The head of JAIC until summer 2020, Lt General Jack Shanahan, had been pushing for JAIC to have its own contracting mechanism and authority, arguing that this was necessary to allow it to keep pace with technology and foreign adversaries, to deliver existing AI-enabled systems to the forces in the next couple of years and to develop systems for AI transformed warfare in the next 20 years.[45]

At the same time a more comprehensive approach towards speeding up the development of AI and other new technologies was being developed by the National Security Commission on Artificial Intelligence (NSCAI). The NSCAI was established by the FY2019 National Defense Authorization Act (NDAA) with the mandate to make recommendations to the President and Congress to "advance the development of AI, machine learning and associated technologies by

[39] DIU Annual Report 2018, p.2.
[40] Defense Innovation Unit, Annual Report 2018, p. 4.
[41] 'About the JAIC', at the JAIC home page, https://www.ai.mil/about.html, visited 20 Sept 2020.
[42] 'DoD Unveils its Artificial Intelligence Strategy', US DoD News, 12 Feb. 2019, https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/
[43] 'About the JAIC', at the JAIC home page, https://www.ai.mil/about.html, visited 20 Sept 2020; and JAIC', Website of Chief Information Officer, DoD, https://DoDcio.defense.gov/About-DoD-CIO/Organization/JAIC/, visited 20 Sept 2020.
[44] 'DOD CIO Remarks at DOD Artificial Intelligence Symposium and Exposition, 10 Sep. 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2342193/dod-cio-remarks-at-dod-artificial-intelligence-symposium-and-exposition/; 'Experts predict artificial intelligence will transform warfare', DOD News, 5 June 2020. https://www.defense.gov/Explore/News/Article/Article/2209480/experts-predict-artificial-intelligence-will-transform-warfare/; and 'Finding Artificial Intelligence Money in the Fiscal 2020 Budget', Bloomberg Government, 28 March 2019, https://about.bgov.com/news/finding-artificial-intelligence-money-fiscal-2020-budget/
[45] 'Defense Department's AI Center seeks own acquisition authorities', NextGov.com, 25 May 2020. https://www.nextgov.com/emerging-tech/2020/05/defense-departments-ai-center-seeks-own-acquisitioauthorities/165657/ ; and 'Experts predict artificial intelligence will transform warfare', DOD News, 5 June 2020. https://www.defense.gov/Explore/News/Article/Article/2209480/experts-predict-artificial-intelligence-will-transform-warfare/

the US to comprehensively address the national security and defence needs of the US."[46] It began its work in in March 2019, with Eric Schmidt as the Chair and Bob Work as Vice Chair and presented its first interim report in November 2019 and its final report in early March 2021. The interim report argued that the manner of adopting AI would have "profound ramifications for immediate security, economic well-being, and position in the world" and identified its importance to the emerging strategic competition with China and others. It showed concern for the threat to the US position as leading innovator and that state and non-state actors could use AI to threaten critical infrastructure, amplify disinformation campaigns and wage war against the US and its allies. In an echo of Cold War rhetoric, it suggested China "has deployed AI to advance an autocratic agenda and to commit human rights violation, setting an example that other authoritarian regimes will be quick to adopt"[47].

Rapid adoption and deployment of AI-enabled systems for the armed forces, was argued to require a fundamentally different approach to arms acquisitions. While the JAIC had been created to help bridge the gap between the large number of existing bottom-up AI projects across the DOD and the required top-down leadership to shift these into established defence programmes, a much more comprehensive approach than the JAIC was needed. This was described as a more rapid, flexible, and interactive approach with top-down leadership and effective coordination to overcome cultural, policy and process barriers to AI adoption.[48] More importantly, to maintain US global competitiveness, the interim report stressed that a nation-wide plan of action was required to maintain US leadership in AI, a "triangular alliance" among government agencies, universities and private companies, as occurred in the early days of the Cold War.[49] While the commercial sector now plays a significant role in AI research, its investments are insufficient for sustaining US advantages. [50] The report then stressed the need for large-scale federal funding of AI R&D and for new mechanisms for channelling the R&D resources. In particular, it argued that the National Science Foundation (NSF) needed a big funding boost, including a doubling of its budget for basic AI research, and that a nationwide AI R&D infrastructure was needed to benefit both national security and economic competitiveness."[51]

In the final report the main recommendations consists of four pillars of action. First, Leadership (by the government). Referring to how the US had created a National Security Council to confront the challenges of the post–World War II era, the Commission recommended the creation of a Technology Competitiveness Council chaired by the Vice President, 'to manage the large-scale development and adoption of AI in all sectors of society, including defense and intelligence communities.' Second, Talent. Arguing that the human talent deficit was the government's most conspicuous AI deficit, the reported proposed the establishment of a new Digital Service Academy and civilian National Reserve to grow tech talent. Third, Hardware. Pointing to the fact that microelectronics power all AI and that the US 'no longer manufactures the world's most sophisticated chips', the report strongly emphasized the need to reevaluate the meaning of supply chain resilience and security and use federal investment and incentives

[46] *Final Report, National Security Commission on Artificial Intelligence*, March 2021, available at https://www.nscai.gov/2021-final-report/

[47] NSCAI, *Interim Report, National Security Commission on Artificial Intelligence*, Nov. 2019, Message from the Chairman and Vice Chairman, pp 1-2, available at https://www.nscai.gov/previous-reports/

[48] NSCAI, *Interim Report, National Security Commission on Artificial Intelligence* (Nov. 2019), pp 31-33, available at https://www.nscai.gov/previous-reports/.

[49] NSCAI, *Interim Report*, p. 24. US federal R&D as a share of GDP was 0.72% in 1953 and peaked at 1.86% in 1964 and by 2017 it had declined to below 1953 level to 0.61%. NSCAI, *Interim Report*, notes 56 and 65, p. 77.

[50] NSCAI, Interim Report, p24.

[51] NSCAI, *Interim Report*, p. 26.

to revitalize domestic microchip fabrication.[52] This referred in particular to US reliance on Taiwan, where, according to the report, the vast majority of cutting-edge microchips are produced. At one of the presentations of the final report, Eric Schmidt argued that the aim should be to revitalize domestic US semiconductor manufacturing and ensure that the US is two generations ahead of China.[53] Fourth, Innovation Investment. The establishment of a national AI research infrastructure and more funding.[54] The main emphasis here was on the huge amount of resources needed to make the biggest AI breakthroughs. While stating that if anything, this report underplays the investments needed, it envisioned hundreds of billions of federal spending in the coming years.[55] The other main point was the need for the federal government to partner with U.S. companies to preserve American leadership and to support development of diverse AI applications that advance the national interest in the broadest sense. The report also pointed to the need to build a secure digital infrastructure across the nation, shared cloud computing access, and smart cities.

In May 2020, bipartisan legislation introduced in US Congress proposed a restructuring of the National Science Foundation (NSF) to focus on AI and other emerging technologies in 10 core areas: AI and machine learning; high-performance computing; quantum computing; robotics and automation; natural or anthropogenic disaster prevention; advanced communication technologies like 5G; biotechnology and genomics; advanced energy technologies; cybersecurity and data management; and material science and engineering. This would be supported by $100 billion funding over 5 years, a tripling of current annual NSF funding, arguing that significant federal tech investment was required if the country wanted to continue leading the worldwide tech arms race, emphasizing the economic and security threats posed by China.[56] While this bill was rejected based on the concern that the strong focus on AI would overshadow the rest of the NSF, a new bill was introduced in March 2021, proposing to more than double the NSF budget over the next 5 years, but without the dominance of AI R&D.[57]

The $2 trillion Biden Infrastructure Plan unveiled in March 2021 included a "major funding push" for federal technology centers and R&D capabilities, requesting $180 billion in new R&D investment, including $50 billion for the NSF and $40 billion for Federally Funded Research and Development Centers (FFRDCs), public-private partnerships that conduct R&D for the US Government.[58]

---

[52] NSCAI, *Final Report*, March 2021, p. 3.
[53] Schmidt, Eric, *Presentation of the Final report of the NSCAI*, Video, 1 March 2021, available at https://www.nscai.gov/
[54] 'And we need more money. In particular, AI R&D so that by 2026 we get $32 billion per year' .Schmidt, Eric, Presentation of the Final report of the NSCAI, Video, 1 March 2021.
[55] NSCAI, Final Report, March 2021, p. 4.
[56] 'Bill proposes restructuring NSF and $100B to focus on tech', Nextgov.com, 27 May 2020, https://www.nextgov.com/emerging-tech/2020/05/bill-proposes-restructuring-nsf-and-100b-focus-tech/165682/; and 'Lawmakers propose dramatic expansion of NSF to boost US technology, American Institute of Physics, 28 May 2020, https://www.printfriendly.com/p/g/a6YuZF
[57] 'House panel offers its plan to double NSF budget and create technology directorate', ScienceMag.org, 26 March 2021, https://www.sciencemag.org/news/2021/03/house-panel-offers-its-plan-double-nsf-budget-and-create-technology-directorate.
[58] 'Biden Infrastructure Plan includes billions for federal funding and research', Next.Gov, 31 Mar. 2021, https://www.nextgov.com/cio-briefing/2021/03/biden-infrastructure-plan-includes-billions-federal-buildings-and-research/173064/; and 'Biden details $2 trillion plan to rebuild infrastructure and reshape the economy', NYT, 2 Apr. 2021, https://www.nytimes.com/2021/03/31/business/economy/biden-infrastructure-plan.html. https://www.nytimes.com/2021/03/31/business/economy/biden-infrastructure-plan.html

Under the Trump administration, there had been a return to focusing on large and increased numbers of traditional types of weapon systems remained an interest in new and emerging technologies and efforts were made to involve commercial technology companies in military projects. An important example of this was the Joint Enterprise Defense Infrastructure (JEDI) initiative for the creation of a cloud infrastructure system. The process of identifying the need, requirements and possibility of developing a defense-wide enterprise cloud enterprise culminated in a tour of big tech companies, including Amazon and Google, in August 2017, by then defense secretary James Mattis and then acting deputy defense secretary Patrick Shanahan. [59] The need for reliance upon commercial companies to accelerate the development of a cloud architecture for warfighting was reinforced by what Shanahan saw within these companies.[60]

In September 2017, Patrick Shanahan produced a memo outlining a strategy to accelerate the DoD's adoption of cloud computing technologies, arguing that this was critical to maintaining the US military's technological advantage. [61] Technologies in areas like data infrastructure and management, cybersecurity, and machine learning were argued to be changing the character of war, but commercial companies were pioneering the technologies in these areas and the pace of innovation was extremely rapid. This was argued to require "aggressive steps to establish a culture of experimentation, adaptation, and risk-taking; to ensure we are employing emerging technologies to meet warfighter needs; and to increase speed and agility in technology development and procurement." [62] The bidding process for the high profile $10 billion JEDI contract was launched in March 2018.

Another example of how the links between the DoD and commercial tech companies continued and if anything strengthened during the Trump administration is the role of Google CEO Eric Schmidt's, whose influence on technological innovation for the military certainly increased significantly. In a portrait by New York Times in May 2020, Schmidt, then also a co-chair of the National Security Commission on AI (NSCAI). was described as 'the prime liaison between Silicon Valley and the military-industrial complex' involved in 'a personal campaign to revamp America's defense forces with more engineers, more software and more A.I.' because the US military "was stuck in software of the 1980s.[63] Assigning an important role like this to someone outside the arms industry represents a significant change to the earlier DoD close and exclusive relations with the established arms producers. The "revolving door" relations, the movement of staff between parts of the MIC, was expanding to include companies outside the established arms industry. A similar example is Joshua Marcuse, a US DoD official, with a background in Booz Allen Hamilton. Together with Eric Schmidt, he launched

[59] Patrick Shanahan (different from Jack Shanahan above) is a former Boeing executive (1986-2017), grew up in Seattle and is still living there. In June 2019, Trump withdrew his nomination (then acting defense secretary) to become the permanent defense secretary and instead named Mark Esper, a former Raytheon executive as defence secretary, 'Shanahan withdraws as Defense Secretary Nominee, and Mark Esper is named Acting Pentagon Chief, NYT, 18 June, 2019, https://www.nytimes.com/2019/06/18/us/politics/patrick-shanahan-defense-secretary.html

[60] Reportedly, in a meeting with Mattis during that visit, the CEO of Amazon, Jeff Bezos, argued that the DoD should "abandon the hodgepodge of 2,215 data centres located in various Pentagon facilities and run using different systems by an array of different companies" and let Amazon replace it with a cloud service. 'How Amazon and Silicon Valley seduced the Pentagon', Propublica.org, 22 Aug 2019, https://www.propublica.org/article/how-amazon-and-silicon-valley-seduced-the-pentagon

[61] US Department of Defense, 'Accelerating Enterprise Cloud Adoption', Memorandum of the Deputy Secretary of Defense, Pentagon, Wash. DC, 13 Sep. 2017. Published at NextGov.com, 9 May 2018. http://www.documentcloud.org/documents/4059163-DoD-Memo-Accelerating-Enterprise-Cloud-Adoption.html

[62] US DoD Memorandum, 13 Sep. 2017 (ibid or note 49).

[63] https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html 2/11/20

the Defense Innovation Board and served as its first Executive Director, helping to establish the JAIC and was among those driving the US DoD towards cloud developments. In 2020, he moved to Google to become the head of strategy and innovation for its Global Public Sector team.[64]

These developments really do represent a break with past state industry relations. While DoD efforts to harness commercial technologies for achieving superiority is not new, there has been a clear change in approach. Unlike earlier efforts there has been a clear attempt to move beyond the established defence industrial base and bring in the major commercial tech companies and entrepreneurs This has left the established defence companies in a new situation, where they have been unable to maintain their position as prime contractors by simply buying in the civil technology and capabilities required, as they have in the past. Instead, they are confronted by civil companies that are more than their match in size and influence. While the defence primes are still managing to get major contracts, this competition my make life more difficult in the future.

4. New technology projects with commercial company involvement

It is not easy to get a clear idea about the results of the DoD change in approach, either in terms of projects and contracts in the targeted new technologies, nor to what extent it has relied on technology access from private venture and commercial companies outside the realm of the established defence contractors. This is because, firstly, the targeted technology fields are broad, focussing on five areas of technology where leading-edge commercial sector capabilities are essential to US military-technical advantage, namely AI, autonomy, cyber, human systems, and space. Secondly, the range of projects and companies to consider is broad, spanning small innovative emerging technology projects with small start-up firms to big multimillion-dollar acquisition projects, with some of the largest technology corporations in the US. Third, and because of this, it is difficult to identify official reports or literature providing a broad and overall assessment of this kind of development.

As regards innovative technology projects, the DIU has continued to act as a major vehicle for accelerating the DoD adoption of innovative commercial technology. By 2019, it had awarded a total of 166 contracts for prototype projects to commercial companies, 72 projects had been initiated and 33 completed since June 2016, when the Commercial Solution Opening (CSO) contracting process was launched.[65] These contracts are small in comparison to regular DoD procurement contracts, with the combined value of $114 million of the 63 contracts awarded during 2019, an average of $1.8 million per contract. They can, however, be important for promoting innovation.

It is difficult to find any easily accessible data on DoD procurement contracts for searches on types of technology or contractor. The DoD News provides daily online announcements on ‘Contracts valued at $7 million or more’.[66] However, there are no easy search paths and it is

[64] ‘DEF’s Board of Directors–Joshua Marcuse’, Defense Entrepreneurs Forum, 1 May 2020, https://medium.com/defense-entrepreneurs-forum/defs-board-of-directors-joshua-marcuse-4e4105846154; ‘Defense Innovation Board Director Moves to Google’, DefenseOne, 1 May 2020. https://www.defenseone.com/technology/2020/05/defense-innovation-board-director-moves-google/165086/

[65] Defense Innovation Unit, Annual Report 2019, p. 10.

[66] US DoD, ‘Contracts: Contracts valued at $7 million or more are announced each business day at 5 p.m.’, https://www.defense.gov/Newsroom/Contracts/

not a list but a compilation of DoD contract announcements to be scanned one-by one. Language is not standardized, so it is necessary to develop several search terms for each type of technology. For example, searches on "artificial intelligence" and "AI" for the period July 2014–September 2020 gave few hits, while a search on "algorithmic" gave several. The low number of hits on AI can also be an effect of what has been described as the fragmented process for AI adoption at the DoD. According to the National Security Commission for AI, by mid-2019, there were over 600 active AI projects across the DoD, each of which was unique in how it was established, fielded and managed. DoD was struggling to shift such bottom-up projects into established programs. None of these obviously made it into the DOD online contract announcements.[67] Finally, the contracts included are of course only prime contracts and subcontractors are seldom mentioned. A search on the names of major tech companies for the period July 2014-September 2020 resulted in no hits for Amazon, Apple, Facebook and Google, 30 hits for Microsoft, and 36 hits for each of IBM and Oracle. The contract for Project Maven (see below) did not mention the name of Google, but only the name of the prime contractor, ECS federal.

Given this lack of easily accessible data, a dataset released in July 2020 showing the links between tech companies and the DoD and federal law enforcement agencies is a major achievement as well as a valuable source of information. It is based on research conducted by Tech Inquiry, a non-profit focusing on technology accountability, investigating the contractual relationships between DoD and Big Tech companies. It was conducted by a former Google research scientist.[68] The survey covers over 30 million US government contracts and subcontracts signed or modified in the past five years, mostly by the DoD and federal law enforcement agencies. The study was able to reveal a large number of subcontracts with private entrepreneurs and commercial tech companies that have not previously been revealed. Silicon Valley companies were found to have thousands of previously unreported subcontracts with the US military and federal law enforcement agencies. Big Tech companies such as Google, Amazon and Microsoft secured more than 5000 agreements with agencies within the DoD and these agencies.[69] One conclusion drawn from the dataset is that in terms of actual contracts, it 'highlights the size advantages of commercial giants like Hewlett-Packard, IBM and Microsoft to navigate government contracting' while smaller cutting-edge-tech firms lag behind.[70]

Considering instead the visible, larger and more high profile projects, one of the early cases of a big commercial tech company working on specifically war-related projects was Google's acquisition in December 2013 of Boston Dynamics, funded by DARPA and DoD to develop robots for military use.[71] This was part of the Google's efforts in the early 2000s to develop a business unit to produce innovative mobile robots, through a series of acquisitions. However, the military versions were not successful. In 2017 Google sold Boston Dynamics to a Japanese

[67] NSCAI, *Interim Report, National Security Commission on Artificial Intelligence* (Nov. 2019), pp 31-33, available at https://www.nscai.gov/previous-reports/.
[68] 'Thousands of contracts highlight quiet ties between Bog Tech and U.S. military', NBC News, 8 July 2020, https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171; The link to the report itself is broken as well as the link techinquiry.org to Tech Inquiry itself.
[69] 'New records show Google, Microsoft, and Amazon have thousands of previously unreported military and law enforcement contracts, *BusinessInsider.com*, 8 July 2020; https://www.businessinsider.com/microsoft-google-amazon-pentagon-law-enforcement-contracts-2020-7?r=US&IR=T; and *NBC News*, 8 July (previous note).
[70] 'Silicon Valley giants – Not start-ups – dominate DoD tech $$', Breakingdefense.com, 10 July 2020, https://breakingdefense.com/2020/07/silicon-valley-giants-not-start-ups-dominate-dod-tech/
[71] A 25-year old robotics design company, spun off from Massachusetts Institute of Technology in 1992. With project such as developing robots to serve as pack mules for soldiers in difficult terrains.

multinational holding company in the field of robotics, SoftBank Group[72].Google was also a commercial participant in Project Maven, although not through a direct contract with the DoD but as a subcontractor to ECS Federal.[73] While Google's contract was relatively small in value terms, it was considered crucial to Google Cloud Platform and an important stepping stone for gaining future government contracts. Google's participation in the project was, however, short-lived due to massive protests by its staff involved in the project at Google Cloud Platform, including leading engineers, some of whom subsequently resigned in protest. One of their arguments was that the technology would inevitably be used without human analysts to perform targeted kills. [74] Following a petition signed by dozens of senior engineers and 4,000 employees in all, Google decided to end its collaboration when the contract was up for renewal in March 2019.[75] While a number of other commercial tech companies have been involved in the project, it is difficult to find information about which ones.[76] The sensitivity of the project in some of the tech companies is demonstrated by the fact that when Apple acquired an AI startup company Xnor.ai, in January 2020, it cancelled the company's work on Project Maven.[77]

In August 2020, the links to warfare of the project became clear, with the announcement that the program office was moving to the Air Force's Advanced Battle Management System (ABMS). This was to allow AI capabilities "to analyze and link data from the vast array of sensors used in battle" to support military operations within the Join All-Domain Command and Control (JADC2), a network-of-networks that aimed to link "every sensor to every

[72] Tobe, F., 'Finally! Google sells Boston Dynamics to SoftBank', The RobotReport, 8 June 2017. https://www.therobotreport.com/finally-google-sells-boston-dynamics-to-softbank/. Today, the company, still based in Boston and with the same CEO, advertises leases and sales of robots for the commercial market, including a robot for disinfection jobs to fight the spread of COVID-19. In 2019, the Massachusetts State Police reportedly started to use a dog robot developed by the company in its bomb squad, 'The Boston Dynamics, robot Dog has joined a bomb squad', PopularMechanics.com, 26 Nov. 2019, https://www.popularmechanics.com/technology/robots/a29994082/boston-dynamics-spot-bomb-squad/.

[73] According to the DoD contract award to ECS Federal related to Maven, the aim was to provide analysis of large data sets 'to provide insight to the warfighter on the tactical edge', *DoD Contract awards*, 15 March 2018, https://www.defense.gov/Newsroom/Contracts/Contract/Article/1467606/

[74] It was a sensitive project, for Google, so much so that the chief scientist for AI at Google Cloud, Fei-Fei Li, instructed staff to be extremely cautious about how they communicated about the project. She urged them to avoid at all costs any mention of AI and instead convey it as a cloud infrastructure project. Google described its work on Project Maven as "non-offensive", but according to the Pentagon, one objective of Maven was to provide video analysis in support of counterinsurgency and counterterrorism and it has been used in the fight against ISIS. Later Fei Fei Li actually became one of the protesters. 'The business of war: Google employees protest work for the Pentagon', New York Times, online, 4 Apr. 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html; and 'What is Project Maven? The Pentagon AI project Google employees want out of', Global News, 5 Apr. 2018, https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/.

[75] 'Google will not renew Pentagon contract that upset employees', New York Times, online, 1 June 2018, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html; and 'Google employee protest: Now Google backs off Pentagon drone AI project', ZDNet, 4 June 2018, https://www.zdnet.com/article/google-employee-protests-now-google-backs-off-pentagon-drone-ai-project/; and New York Times, 4 June 2018 (note above).

[76] 'As Google quits controversial Project Maven, mystery deepens over role of other tech firms', FastCompany.com, 2 Apr. 2018, https://www.fastcompany.com/40580354/as-google-quits-controversial-project-maven-mystery-deepens-over-role-of-other-tech-firms.

[77] 'Apple cancels preexisting military drone Pentagon contract after acquiring AI company', FastCompany.com, 30 Jan. 2020, https://www.fastcompany.com/90458102/apple-cancels-preexisting-military-drone-pentagon-contract-after-acquiring-ai-company

shooter" across air, land, sea, space and cyber."[78] Indeed, the Air Force's assistant secretary for acquisitions, technology and logistics, noted it is now "the most advanced warfighting system development."[79] The Joint Artificial Intelligence Center (JAIC) was partly modelled on Project Maven but expanded into new fields and military operations within the Pentagon's broader objective of making AI a centerpiece of its weapon strategy. Director of Project Maven, Jack Shanahan was also the inaugural JAIC director.[80] Since then a number of large technology contracts have been opened for competition or awarded in artificial intelligence and in the related field of cloud computing. The largest so far is an $800 million contract for AI-enabled products awarded to Booz-Allen Hamilton in May 2020. [81]

Cloud computing projects

The most visible tech projects emerging since 2018 are in the area of cloud computing, both because of their large size and because of the involvement of the big commercial tech companies. Interestingly, it was the risk-averse CIA that had taken the first step to contract out part of its activities to the commercial technology industry, with a $600 million contract to Amazon for a cloud enterprise adoption project in 2013.[82] In 2020, the CIA was reported to be developing a multi-billion follow-on cloud computing project.[83] The largest DoD initiative is the JEDI project aiming to develop a comprehensive cloud enterprise system for overall DoD activities, under a contract potentially worth $10 billion over 10 years. It opened for bidding in July 2018, with bids submitted by Amazon, IBM, Microsoft and Oracle.

Another multi-billion cloud computing project to emerge during 2019 was the Defense Enterprise Office Solutions (DEOS), a 10-year contract worth up to $7.6 billion, was to provide cloud-based office services, such as email, word processing and file sharing, for all military branches.[84] The Marine Corps was to use this software for small units training 'to operate in the modern battlefield's disconnected, degraded and low-bandwidth environment'. [85] The contract, which was expected to be won by Microsoft, was initially awarded to a team led by General Dynamics, through its recently acquired subsidiary, CSRA, partnering with Dell

[78] 'Air Force moving Project Maven into Advanced battle Management System portfolio', FedScoop.com, 10 Aug. 2020, https://www.fedscoop.com/project-maven-air-forces-advanced-battle-management-system/
[79] Fedscoop, 10 Aug 2020 (note above).
[80] 'The Pentagon wants to expand its controversial Project Maven AI initiative', Venture Beat.com, 29 May 2018, https://venturebeat.com/2018/05/29/the-pentagon-wants-to-expand-its-controversial-project-maven-ai-initiative/
[81] 'Pentagon's AI Center awards $800M contract through GSA Center of Excellence Program', NextGov.com, 18 May 2020, https://www.nextgov.com/emerging-tech/2020/05/pentagons-ai-center-awards-800m-contract-through-gsa-center-excellence-program/165479; and US DoD, Newsroom, Contracts, *Joint Artificial Intelligence Center,* 18 May 2020, https://www.defense.gov/Newsroom/Contracts/Contract/Article/2190758/.
[82] 'The details about the CIA's deal with Amazon', *The Atlantic*, 17 July 2014, https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/ ; and 'CIA tech official calls Amazon cloud project 'transformational', Bloomberg.com, 21 June 2018, https://www.bloomberg.com/news/articles/2018-06-20/cia-tech-official-calls-amazon-cloud-project-transformational
[83] 'The CIA wants to upgrade its cloud tech without DoDs JEDI drama',Techcrunch.com, 7 Feb. 2020, https://techcrunch.com/2020/02/07/the-cia-wants-to-upgrade-its-cloud-tech-without-DoDs-jedi-drama; and 'CIA reportedly seeking to hire multiple providers for new cloud computing contract', siliconangle.com 5 Feb. 2020, https://siliconangle.com/2020/02/05/cia-seeking-hire-multiple-providers-new-cloud-computing-contracts/
[84] 'Analysts: Pentagon's multibillion-dollar DEOS contract is guaranteed for Microsoft', NextGov.com, 28 Mar. 2019, https://www.nextgov.com/it-modernization/2019/03/analysts-pentagons-multibillion-dollar-deos-contract-guaranteed-microsoft/155901/
[85] 'General Dynamics wins huge military cloud contract', Toolbox.com, 13 Dec. 2019, https://it.toolbox.com/article/general-dynamics-unit-wins-huge-military-cloud-contract

Marketing and Minburn Technology Group. However, protests by another bidder, Perspecta, led the DoD to reassess its decision and a final decision had not yet been made by June 2020. A third large cloud computing project, was announced in May 2020, this time a DIU contract to Google Cloud to build a secure multi-cloud management solution to detect, protect against, and respond to cyberthreats.[86]

Although the contract for JEDI and other cloud computing projects are among the largest DoD contracts to commercial tech companies, they are still substantially smaller than the largest DoD contracts for traditional weapons systems with established defence contractors. In fiscal year 2020, the total value of DoD contracts was $421 billion and the top defence contractor that year, Lockheed Martin were awarded DoD contracts at a total of $75 billion.[87] Individual DoD contracts at the billion-dollar level are not unusual. The significance of the cloud computing contractors to commercial tech companies is rather the large size to a company outside the group of established defence contractors. This, in turn, reflects the fact that cloud computing had become a major growth area, with the growth of the internet, and that the military sector was well behind civil technology, capacity and capability.

The growing cloud computing market

Any business that provides or uses online services needs some system for storing and managing data and this can be expensive and time-consuming, drawing resources from their core activities. This has resulted in a large and rapidly growing commercial market for cloud services and a high level of innovation. The worldwide global public (i.e. available over the Internet) cloud services market is forecast to grow from $242 billion in 2019 to almost $260 billion in 2020 and $364 billion in 2022. [88] The market consists of six main segments. First, infrastructure as a service (IaaS), the most advanced which develops the architectures for cloud computing and was worth $44 billion in 2019 and is forecast to grow to $81 billion by 2022. Second, platform as a service (PaaS), that provides storage on the cloud. Third, Software as a service SaaS, that provides software and support on the cloud, which is the largest area and worth $102 billion in 2019. Over time, the service provision has developed, with another three segments: Business Process as a service (BPaaS), Cloud management and security services, and Desktop as a service (DaaS).[89] The security services part of DaaS is expected to grow rapidly as threats develop. Cloud users need firewalls and security services, that balance cost and ease of use against risk and this will vary depending on the nature of the company, its products and customers. Security will, of course, be disproportionately important for any defence clouds. So, it is an area of dynamic change and it is clear that its development provides important opportunities, but also considerable security threats, particularly for defense related applications.

Infrastructure as a service (IaaS), the dynamic segment that is most relevant for the DoD saw global sales increase by 37% in 2019. Amazon established its cloud service business Amazon Web Services (AWS) in 2006 and has led the market since it began to offer IaaS in 2008. The

[86] 'Defense Innovation Unit Selects Google Cloud to Build Secure Cloud Management Solution, Google Press release, 20 May 2020, https://cloud.google.com/press-releases/2020/0520/defense-innovation-unit; and 'Google lands multicloud cybersecurity projects with the DOD', Siliconangle.com, 20 May 2020, https://siliconangle.com/2020/05/20/google-lands-multicloud-cybersecurity-project-DoD/

[87] 'Top-100 Defense contractors 2020', http://www.fi-aeroweb.com/Top-100-Defense-Contractors.html

[88] 'Gartner forecasts worldwide public cloud market revenue to grow 6.3% in 2020'. Press release, Gartner, Stamford, Conn., 23 July 2020. https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

[89] 'Gartner, Press release, 23 July 2020 (note above).

strong growth of the market led other big tech companies to rapidly develop their capacities. Google formed its Google Cloud Platform in 2016, Microsoft announced its Microsoft Azure business in 2017. [90] Amazon remains the market leader, with 45% of the global market in 2019, followed by Microsoft 17.9%, Alibaba (China) 9.1%, Google 5.3% and Tencent (China) 2.8%.[91] In Software as a Service (SaaS), the global market leaders are Salesforce, Oracle and SAP, while in multi-cloud hybrid provisions, which combine several market segments, the market leaders are IBM, Dell Technologies and Hewlett-Packard Enterprise and VMware. In 2019, IBM acquired open-source software enterprise Red Hat for a record sum of $34 billion, to integrate in its hybrid cloud division, reportedly in an effort to compete with Amazon and Microsoft.[92]

DoD interests in cloud computing

While the DoD has the same kind of needs as the commercial users, when moving their activities into cloud processes (as exemplified by DEOS) they may well have more or different security concerns. In addition, cloud computing services are expected to have a significant impact on the warfighting operations of the armed forces and their operations in the battlefield. In principle, the outcome of products such as JEDI, could see the military having real time access to comprehensive data, information and analytical tools through cloud systems, even in isolated areas and conflict zones. Once online they would have access to the facilities of the cloud which would help to clear the 'fog of war' and make advanced weapons systems easier to use successfully. [93] This is likely to make security concerns more onerous than in civil uses. That said, the cyber attacks on individual, groups, political parties and business internets by foreign governments suggest that security and intelligence are going to be important. Indeed, the DoD may end up becoming involved in organising cyber defences for the civil sector. Having recognised the potential importance of cloud services, the DoD also recognised the need to engage with the tech companies. The existence of reliable external cloud operators in the civil sector has become extremely popular as firms and organisations saw the benefits of outsourcing a big part of data management and storage.

Cloud providers can keep the costs they charge down by economies of scale and locating their services across the world, as they have no reason to be in the country where the data is. For example, there is a large Amazon cloud base in Cape Town. This potential for internationalization may be of concern for the use of such services in the defence and security areas. Amazon is even trying to expand its cloud universe to space.[94]

---

[90] 'Gartner says worldwide IaaS public cloud services market grew 37.3% in 2019, Gartner, Press release, Stamford, 10 Aug. 2020, https://www.gartner.com/en/newsroom/press-releases/2020-08-10-gartner-says-worldwide-iaas-public-cloud-services-market-grew-37-point-3-percent-in-2019

[91] 'Gartner, Press release, 10 Aug. 2020 (note above).

[92] For a more comprehensive overview of the cloud providers, see 'The top cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players', ZDNet, 11 May, 2020, https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/

[93] 'DoD Officials highlight role of cloud infrastructure in supporting warfighters', DoD News, 14 Mar. 2018, https://www.defense.gov/Explore/News/Article/Article/1466699/dod-officials-highlight-role-of-cloud-infrastructure-in-supporting-warfighters/

[94] 'Amazon launches space push to drive cloud-computing growth': ASW's move comes during a multiyear surge in U.S. military and civilian agency spending on space projects. Wall Street Journal, 30 June 2020, https://www.wsj.com/articles/amazon-launches-space-push-to-drive-cloud-computing-growth-11593489660 ; 'Amazon Web Services is creating its own space force for cloud computing', GeekWire, 30 June 2020. https://www.geekwire.com/2020/amazon-web-services-creates-space-force-cloud-computing/ ; and 'Amazon looks to space to expand its cloud-computing business: Amazon Web Services announces a new aerospace and

Company interests in DoD contracts

In the JEDI process, two of the Big Five tech companies in the US—Amazon and Microsoft—were competing and initially also Google. There was also one other major tech company, Oracle, and one of the traditional defence contractors, IBM. The two other Big Five companies, Apple and Facebook, did not have the required capability. Google, dropped out of the bidding process on 8 October 2018, 4 days before the deadline for submitting bids. It stated that it believed this work would conflict with its corporate principles and because it believed it might not hold all of the necessary certifications.[95]

Throughout the highly contested bidding process, indeed even before it was formally started, Amazon was the expected winner, as it was seen to have the strongest cloud infrastructure capabilities in AWS. It also had the strongest share of the US cloud services market, had been authorized with the required security certifications, had been working on a similar $600 million contract providing cloud services since 2013 to the CIA, and was also working on other smaller US government cloud services contracts. IBM and Oracle, whose database business was threatened by the rise of cloud computing, launched several protests over the contracting process before they had to give up in April 2019. One of the major allegations was that the design of the process favoured AWS. However, in October 2019, the DoD announced that the contract had been awarded to Microsoft. Amazon immediately protested that there was a flaw in the assessment process. Despite Amazon's failure, Oracle, continued its legal accusation. It claimed that top officials were conspiring to give Amazon a long-term monopoly on the military's information-technology infrastructure**[96].** The DoD requested some time to reconsider its decision and the Court of Federal Claims granted AWS's request for a temporary restraining order on Microsoft moving forward, followed by a judgement allowing the military a period of remand to consider aspects of how it evaluated the vendor bids. After several delays, requested by the DoD for its reassessment, in early September 2020, the DoD reaffirmed its decision to award the contract to Microsoft.[97] Amazon responded the same day in a blogpost by AWS, saying that AWS would 'continue to protest this politically corrupted contract award.'[98] In fact, Amazon has maintained since the day it lost the JEDI contract that the decision-making process had been influenced by presidential interference, because of his personal antipathy of Amazon CEO Jeff Bezos. In particular, Bezos owns the Washington Post, which Trump had accused of spreading fake news. [99]

---

satellite unit', cnet, 30 June 2020, https://www.cnet.com/news/amazon-looks-to-space-to-expand-its-cloud-computing-business/ .

[95]'Google drops out of contention for a $10 billion defense contract because it could conflict with its corporate values, Business Insider, 9 Oct. 2018, https://www.businessinsider.com/google-drops-out-of-10-billion-jedi-contract-bid-2018-10?r=US&IR=T ; and 'Google drops out of Pentagon's $10 billion cloud competition, Bllomberg.com, 8 Oct. 2018, https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition

[96] https://www.washingtonpost.com/business/2019/11/08/oracle-presses-ahead-with-pentagon-cloud-lawsuit-despite-amazons-loss/

[97] 'Pentagon sticks with Microsoft for cloud computing contract, New York Times, 4 Sep. 2020, amazon.html?campaign_id=2&emc=edit_th_20200906&instance_id=21955&nl=todaysheadlines&regi_id=29727840&segment_id=37531&user_id=3b8641a55b5fa187cd56a87f5c91463b

[98] 'Pentagon awards JEDI cloud contract to Microsoft for the second time, NextGov 4 Sep. 2020, https://www.nextgov.com/it-modernization/2020/09/pentagon-awards-jedi-cloud-contract-microsoft-second-time/168259/

[99] 'Microsoft Wins Pentagon's $10 Billion JEDI Contract, Thwarting Amazon', NYT Online, 25 Oct. 2019, https://www.nytimes.com/2019/10/25/technology/DoD-jedi-contract.html ; 'Microsoft Wins Pentagon Deal

Ethical concerns

An interesting question is whether the move of the civil tech companies into projects of direct relevance for military warfighting will be constrained by internal resistance based on ethical considerations. For example, new ways of deploying artificial intelligence in weapons systems and the growth in the development of autonomous weapons are bringing tech companies closer to the front line. [100] However, while the commercial tech companies do face potential constraints internally, they do not seem to be too limiting. Google, with its motto of "don't be evil", abstained primarily for ethical reasons from the Maven project. It was strongly pressured by its staff, who also pressed management to take an official position to stay out of any business designed to cause or directly facilitate injury to people. [101]. At the same time, however, the Google leadership continued to cultivate relations with top Pentagon officials and to strongly commit the company to US defence efforts. The strong opposition groups within the staff left the company, and in May 2020 Google was awarded a multimillion DoD cloud contract.[102] Google also stated that it would have submitted a proposal for part of the JEDI project if it had been a multi-vendor arrangement rather than a "winner-take-all contract".[103] Some indication of the changing attitudes of management might be reflected in the history of Google's "Don't be evil" motto. When Google underwent its corporate restructuring in 2015, the resulting conglomerate, Alphabet Inc., took "Do the right thing" as its motto. Google, now a subsidiary of Alphabet retained "Don't be evil" in its corporate code of conduct, but in April 2018 it was removed from the code of conduct's preface to its last sentence.[104]

In contrast to Google, Microsoft has long taken a strong stance in support of US military activities, while allowing staff with conflicting views to move from work on defence projects to others. Such ethical issues did not seem to be a problem for Amazon, possibly because with its project for CIA, starting in 2013, they have been involved in the security sector for a while. Though the tech industry has a reported tradition of giving their skilled employees flexibility, a voice and accountability, such lauded labour relations are now being questioned, with the industry's rise to power and the lack of visibility into their operations.[105] The fact that there are few signs of unrest over defense-related deals at Amazon and Microsoft should maybe not be a surprise, as Silicon Valley's history is somewhat linked to military work. The internet itself,

---

Over Amazon, NYT, 26 Oct, 2019, Section A, Page 1; and 'Pentagon awards $10-billion 'war cloud' deal to Microsoft, snubs Amazon', Deutsche Welle, 26 Oct 2019.

[100] 'Report: Companies like Amazon and Microsoft are 'putting world at risk' of killer AI', Artificial Intelligence News, 22 Aug. 2019, https://artificialintelligence-news.com/2019/08/22/report-companies-amazon-microsoft-world-risk-ai/

[101] According to Google's AI principles, "the company, will not design or deploy AI in weapons or other technologies designed to cause or directly facilitate injury to people; or in technologies that gather or use information for surveillance violating internationally accepted norms; or technologies for any purpose that contravene widely accepted principles of international law and human rights." Google, *Responsible Development of AI*, p. 4.

[102] 'Google cloud wins multimillion-dollar Pentagon cybersecurity contract', NextGov. 20 May 2020. https://www.crn.com/news/cloud/google-cloud-wins-multimillion-dollar-pentagon-cybersecurity-contract ; and 'What Google's new contract reveals about the Pentagon's evolving cloud '. Defense One, 20 May 2020. https://www.defenseone.com/technology/2020/05/what-googles-new-contract-reveals-about-pentagons-evolving-clouds/165524/

[103] 'Google: Here's why we're pulling out of Pentagon's $10bn JEDI cloud race', zdnet.com, 9 Oct. 2018, https://www.zdnet.com/article/google-heres-why-were-pulling-out-of-pentagons-10bn-jedi-cloud-race/

[104] https://time.com/4060575/alphabet-google-dont-be-evil/. See also Wikipedia on "Don't be evil".

[105] 'The line between Silicon Valley and Tech', Wired, 21 May 2018. https://www.wired.com/story/the-line-between-big-tech-and-defense-work/

while a civil innovation, owes a lot of development to a project at the Defense Advanced Research Projects Agency (DARPA), and many tech firms benefited from the generous defense spending during the Cold War. More recently, however, some tech firms obscured their government ties, particularly after the 2013 revelations of government surveillance from former National Security Agency contractor Edward Snowden[106].

Interestingly, in February 2020, the DoD adopted its own set of five ethical AI principles. [107] According to these, the DoD's use of AI systems should be responsible, equitable, traceable, reliable and governable. [108] These principles were based on recommendations by the Defense Innovation Board after a 12-month study. Arguing that artificial intelligence 'is expected to affect every corner of the Department and transform the character of war', the Board proposed the adoption of five AI Ethics Principles to help guide, inform, and inculcate the ethical and responsible use of AI (in both combat and non-combat environments) by the DoD help maintain technological and ethical advantage. [109] As a basis for its recommendations, the Board had made a survey of other AI Ethics Principles for the public sector, including by other countries and by international organizations (such as the European Commission and OECD) as well as by the private sector (such as Google, IBM, Microsoft and OpenAI), civil society groups, professional societies and multi-stakeholder groups. In particular, they referred to those developed by the 2019 United Nations Group of Governmental Experts on Lethal Autonomous Weapons, convened under the Convention on Certain Conventional Weapons.[110]

So, there are clearly profound changes taking place. What is interesting is the degree of change the DoD is undertaking to develop cloud and IT technologies with the tech companies. The enthusiasm of the response by the companies is also striking. They clearly see the projects of value and not as a threat to their continuing as successful civil companies, which may result from their being inveigled into the MIC. It is also interesting to see how the reputation of 'progressive' tech companies seems to have little effect on their engagement with the DoD, aside from some staff opposition that seems easily dealt with. The tech companies have quickly adopted the practices of the arms industry procedures, such as using the opportunity to appeal through state federal court procurement appeal system. There is also evidence that they have started to act in non standard ways, for commercial tech companies. Individuals have been moving between the tech companies and the Pentagon as part of the 'revolving door' and they are undertaking considerable lobbying activity. This behaviour formed part of the appeals by Oracle against being excluded from the JEDI process. It suggests the tech firms a§re learning how to operate within the state and just within the law rather fast. Indeed, if anything, they seem less encumbered by the Pentagon regulation than the established defence companies[111]. It will be interesting to see whether they will start to engage in competition for projects not

[106] Guardian Snowden pages www.guardian.com
[107] 'DoD unveils how it will keep AI in check with ethical principles'. *Federal News Network*, 25 Feb. 2020. https://federalnewsnetwork.com/defense-main/2020/02/DoD-unveils-how-it-will-keep-ai-in-check-with-ethics-principles/
[108] 'AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense', Defense Innovation Board, Oct. 2019, p. 8; and 'AI Principles: recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. Supporting Document'. Defense Innovation Board, Oct 2019.
[109] 'AI Principles: recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. Supporting Document'. Defense Innovation Board, Oct 2019, p. 3.
[110] 'AI Principles: recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. Supporting Document'. Defense Innovation Board, Oct 2019, pp. 73-74.
[111] See the details in "How Amazon and Silicon Valley Seduced the Pentagon" — ProPublica https://www.propublica.org/article/how-amazon-and-silicon-valley...

involving JEDI type procedures and in direct competition with the established defence companies.

5. Changing DIB and MIC

It does appear to be very interesting times for the DIB and the MIC, which have seen considerable change over the years, but also a remarkable degree of continuity, reflecting the specificities of the DIB left over from the Cold War. So far, the challenges faced have usually seen the traditional prime contractors come out on top, but they have not had to deal with the sort of challenges they face now from the large and efficient tech companies. The two groups of companies are experienced in very different environments. The arms companies generally deal with long generation times, very different to the quick procurement and short life cycles in the civil tech sectors. Low margin high volume producers like Amazon, which has also tended to plough back profits into investments, are very different to the traditional arms companies who are high margin low volume producers and often offer high dividends. DoD contracts offer safe and generous returns, but it usually expects ownership of the intellectual property, which does not fit with the commercial tech model (Smith, 2009).

These commercial tech companies also look rather different to the arms companies. Table 1 shows financial and employment data for the five commercial technology companies initially involved as bidders for the JEDI contract. All these five companies are currently involved in various smaller or larger bidding processes or ongoing projects for the DoD. They are large companies, with total revenues in the range of $40–281 billion. In comparison, the top 10 arms-producing and military services companies (apart from Boeing, which has exceptionally large revenues) had total revenues in 2018 in the range of $27.1–53.8 billion and arms sales in the range of $23.4–47.3 billion, as shown in Table 2. Defence firms have strikingly lower R&D expenditures, but this reflects that much of their R&D will have been covered by the DoD[112].

There have been changes in the relationship between company-funded and state-funded R&D. In the 1980s, a huge share of national R&D was spent by military contractors and funded by the state (customer-funded), this was the ‘baroque arsenal’ period of expensive, poor performance and overspecified weapon systems period (Kaldor, 1981). This has rapidly dropped off and by the early 2010s, military R&D was a much smaller part of national R&D, with instead tech companies leading the way (Dunne et. al., 2020)

With the end of the Cold War, the United States was the largest spender worldwide by a large margin. While cuts were made, the increases in US spending in the late 1990s and early 2000s further widened the gap. The US accounted for more than 60 percent of global spending on military R&D by 2004. As Table 3 shows, by 2005 defence R&D was 49% of the government budget allocation for R&D (GBARD). It did then decline, but in recent years has been increasing. The UK is next highest in the OECD with 23.5% in 2005 declining to 16.7 then declining to 15.2 in 2017. The OECD overall figures are higher than the UK but followed a similar pattern. The EU (28) are much lower.

Military R&D had also declined as a share of total R&D due to major increases in civilian expenditure. Even in the US, civilian spending is now substantially larger than military

[112] Defence companies are more risk averse, investing in R&D when they get indications someone will buy the end products. Commercial tech companies need to innovate to survive.

spending and most of the civilian R&D is privately funded. Increasingly civilian R&D occurred in technology lines important for the production of military goods and there was a major shift towards the military use of technologies driven by civilian R&D, particularly in electronics. The success of civilian technology production thus led to a move away from the traditional cultures of technology generation in the military sector. While globally, policy approaches ranged from supporting military R&D to provide major technology advances to limiting the role of military R&D to filling gaps left by civilian R&D (Brzoska, 2006). Until relatively recently, the US still remained reliant on military R&D, but as we have suggested, that may be changing.

US federal R&D as a share of GDP was 0.72% in 1953, peaked at 1.86% in 1964 and by 2017 at 0.61%, it had declined below the 1953 level.[113] The Biden Administration, inaugurated in January 2021, is committed to a significant increase in federal research and science. In his first formal press conference as President, Joe Biden stated that while today, the US invests 0.7% of GDP 'in pure research and science' he would 'make sure that we invest closer to 2%', though his comment came without a timeframe. [114] The Biden administration has also indicated that they will take a broader approach to the development and adoption of new and emerging technologies for the military, by a heavy federal investment in such technologies more broadly and collaborate with the commercial sector, for the benefit of both the global competitiveness of the US economy and of the US military.[115]

[113] NSCAI, *Interim Report, National Security Commission on Artificial Intelligence,* Nov. 2019, p. 77, notes 56 and 65.
[114] 'Biden commits to investing 'closer to 2% of GDP in science research, NextGov.com, 25 Mar- 2021, https://www.nextgov.com/cio-briefing/2021/03/biden-commits-investing-closer-2-gdp-science-research/172933/
[115] 'Biden Infrastructure Plan includes billions for federal funding and research', Next.Gov, 31 Mar. 2021, https://www.nextgov.com/cio-briefing/2021/03/biden-infrastructure-plan-includes-billions-federal-buildings-and-research/173064/; and 'Biden details $2 trillion plan to rebuild infrastructure and reshape the economy', NYT, 2 Apr. 2021, https://www.nytimes.com/2021/03/31/business/economy/biden-infrastructure-plan.html. https://www.nytimes.com/2021/03/31/business/economy/biden-infrastructure-plan.html

Table 1. Five major commercial technology companies competing for large DoD cloud computing contracts, financial and employment data, 2019

	Amazon	Google[b]	IBM	Microsoft	Oracle
Revenues	281	161	77	126	40
Net income	11.6	41.7	9.4	39.2	11.0
Share of net income in revenues (%)	*4.1*	*25.9*	*12.2*	*31.1*	*27.5*
Employees	798,000	114,00	352,600	144,000	136,000
R&D exp.	35.4	26.0	6.0	16.9	6.0
Share of R&D exp. in total revenues (%)	*12.6*	*16.1*	*7.8*	*13.4*	*15.0*
Cloud business unit	Amazon Web Services	Google Cloud	IBM Cloud	Microsoft Azure	Oracle Cloud
Cloud revenues	35.0	8.9	21.2	44.7	32.6
Share of cloud in total revenues (%)	*12.5*	*5.5*	*27.5*	*35.5*	*81.5*

Notes:
Figures are in US$ billion.
[a]Figures are as reported by the companies in their annual reports. Figures for cloud revenues are uncertain for several reasons, notably because they may not be comparable across companies. Information for IBM is particularly uncertain. IBM claims to have a long history of competence in cloud computing.
[b]Figures are for Google (not for its parent company Alphabet).
Sources: Company annual reports and company 10-K reports.

Table 2. Top 5 US defence companies, financial and employment data, 2018

	Lockheed Martin	Boeing	Northrop Grumman	Raytheon	General Dynamics
Arms sales	47.3	29.2	26.2	23.4	22.0
Revenues	53.8	101.1	30.1	27.1	36.2
Share of arms sales in total revenues (%)	*88*	*29*	*87*	*87*	*61*
Net income	6.2	10.5	3.2	2.9	3.3
Share of net income in revenues (%)	*11.5*	*10.4*	*10.6*	*10.7*	*9.1*
Employees (year-end)	105,000	153,000	85,000	67,000	105,600
R&D exp., company-funded	1.3	3.3	0.8	0.8	0,5
R&D exp., customer-funded	. .	. .	. .	. .	. .
R&D exp., total	. .	. .	. .	. .	. .
Share of company-funded R&D exp. in total revenues (%)	*2.4*	*3.2*	*2.5*	*3.1*	*1.4*

Notes:
Figures are in US$ billion.
The top defence contractors have a large amount of R&D expenditure funded by the DoD in addition to what is funded by the companies themselves. However, these amounts are not reported in the annual reports.
Sources:
Arms sales: Fleurant, A., et al., The SIPRI Top 100 arms-producing and military services companies, 2018, SIPRI Fact Sheet, Stockholm, Dec. 2019, available at https://www.sipri.org/publications/2019/sipri-fact-sheets/sipri-top-100-arms-producing-and-military-services-companies-2018.
All other data: Company annual reports and company 10-K reports, as well as for comparative purposes:
Net income: Macrotrends.net, https://www.macrotrends.net/stocks/charts/LMT/lockheed-martin/net-income
Employment: macrotrends, https://www.macrotrends.net/stocks/charts/GD/general-dynamics/number-of-employees
Company-funded R&D exp: Aeroweb, Forecast International, online: http://www.fi-aeroweb.com/Aerospace-Defense-Companies.html

Table 3. Defence budget R&D as % total Government R&D budget (GBARD)

	2005	2014	2015	2016	2017	2018
US	49.1	41	41.6	42.7	43.5	46.3
Eu28 (est)	10.2	4.7	4.5	4.3	4.7	
OECD	26.1	17.7	18.0	18.8	19.2	
UK	23.5	16.7	16.4	15.8	15.2	

Source: OECD Main Science and Technology Indicators -accessed 14/12/20

A trademark of the big tech companies is that they are investing a considerable share of their revenues in R&D, with four of the five spending more than 10% of their revenues on R&D[116]. In fact, in 2017, Amazon was the top R&D spender among all US corporations, with an R&D budget of $23 billion (partly to boost its cloud computing business) followed by four other technology companies: Google-Alphabet, Intel, Microsoft and Apple, collectively these five spent $76 billion on R&D. By 2019, Amazon had increased its R&D budget by 54% to $35 billion and Google by 60% to $26 billion. Cloud business accounts for a major share of revenues, in particular for Oracle, Microsoft and IBM, which are active in several cloud computing market segments. Amazon and Google have a lower share of cloud revenues, but are focused strongly on one market segment (IaaS). In addition to these big tech companies, there are also a large number of smaller firms involved in this area, including many startups marketing innovative ideas and concepts. The market is also developing rapidly, with intense merger and acquisition activity, as shown by the annual lists of "Biggest technology acquisitions" published by Computerworld.com[117].

It is worth noting that a lot of defence contracts are likely to continue with the old model and be dominated by the established firms. However, in the areas of IT and the new technologies, where the DoD seeks to benefit from civil technological innovations, they are attempting to encourage the type of companies that don't bother with the defence sector because of its nature. In the civil tech sector, small firms are used to getting venture capital to innovate and may be successful or not and may get bought up by larger companies if successful. Smaller companies are often part of a stable run by entrepreneurs. They set up many companies, with venture capital focusing on particular initiatives or innovations, expecting both failures and success. The success is expected to pay for the failures and more. This is rather different to the DoD projects in which companies get safe returns when awarded contracts but are not going to strike it rich.

The development of the Defense Innovation Unit (DIU) is part of an attempt to make DoD contracts more encouraging for smaller tech companies. Its engagement with more than just the contracts is indicative of changing attitudes in DoD and wider thinking. It applies beyond the IT industry innovations focused on in this paper but is not without precedent. The arms industry primes (large defence companies) generally started out as innovative high tech civil companies, with support from government. For a while there have been cycles of attraction/repulsion between tech firms and the military, with DARPA having rather different attitudes to the rest of the DoD. With hardware, the differences between the established arms

[116] Though, it should be borne in mind that many of the technologies being developed had their genesis in blue sky research funded by the State.

[117] https://www.computerworld.com/article/3412327/notable-technology-acquisitions-2019.html Accessed 16/11/20

companies, with their customized systems and components, and companies serving mass civil markets is stark. This was not such a problem in the early days of integrated circuits, but once economies of scale became important and the commercial market grew, companies such as Intel did not want to bother with specific military chips and be involved in procurement practises, preferring to simply sell their products. This reflected the increasing 'spin in' of civil projects and was also apparent in software and IT services (Smith, 2009; Amara and Franck, 2020).

These changes may represent a step change in the way that R&D is done in the defence sector, with more the flexible approach of DARPA taking over from the traditional approach of DoD (Bonvillian et al, 2019). This interesting area is where the new technologies and the old arms production technologies interact, bringing very different cultures together. Certainly, military procurement rules, bureaucracy and red tape have acted as barriers to entry to the defence market and the proposed changes with DIU etc are looking to move away from this. While it is only for specific areas at present, it could represent a more general change and start to be applied to innovation in the core areas. It is also clear that the military, with PMCs, and NASA, with SpaceX, are now willing to use commercial firms outside traditional aerospace primes to do what they did in house in the past [118].

Unlike in previous innovations, such as the RMA, the established defence firms are unlikely to be able to simply take companies over to gain capabilities. They have bought start-ups, but larger tech companies are simply too large and powerful and the smaller companies bring rather different cultures but may be vulnerable. Similarly, they can't really use their power of mastery of red tape and the revolving door and contacts etc. to dominate, as they have in the past, as the attitude of the defence department and procurement practices have clearly changed. The tech companies now have close relations with the DoD and people from the sector have become key advisers to the DoD, though so far only on innovative technologies contracts with the commercial tech companies. So there will still be plenty of work for the established arms producers and they retain clear advantages in the more established sectors. The tech companies may also need the support and/or involvement of the defence companies to adapt their technologies to military use.

That said, with the changes in technology a large part of defence spending is likely to go to the areas that the new tech companies are in. They are winning contracts and these are potentially large contracts. One question is how important such contracts will be for the newcomers and what their reasons are for involvement in the sector: opportunism or strategy. If opportunism, it may have little impact on the companies and they would maintain their commercial focus and nature. If strategy, they may become increasingly focused on DoD contracts, become an integral part of the DIB and change their nature. They may establish special sections to deal with DoD contracts, which some already have for federal contracts. This was done by some companies involved in defence work in areas such as electronics, during the Cold War, because of the very different nature and dynamics of the two markets (Dunne, 1995).

Interestingly, Amazon set up cloud services for its own internal use and it was only later that it realized the potential to offer these to outsiders. As its cloud services developed, they became Amazon's profit engine, accounting for 58.7% of Amazon's operating profit in 2018, increasing

[118] https://observer.com/2020/06/how-spacex-crewed-nasa-changes-spaceflight-forever/

to around 67% by the 4th quarter 2019.[119] Amazon is a company used to dealing with complex logistics and large amounts of data and working with low margins, so it is a difficult company to compete with. The only real competitors are companies similar to itself, as it would be almost impossible for a traditional defence producer, used to long development, small orders and high margins, to offer a similar service/product at a competitive price.

While it is clear that the commercial market is very different from the defence one, the driver for the companies is the same, profit. They are in fierce competition for government contracts in the field, as the potential future central, regional and local government markets are huge and profitable. Involvement in the present competitions will open up the future ones to companies and contribute to their reputation as capable providers of large, complex and secure cloud services, which will assist in the wider market, domestic and international. While the commercial companies may have concerns in taking on DoD contracts, with their lack of knowledge of the structure of that market, there is little risk. They are being asked to provide something they have already developed and so have confirmed profit. They are likely to consider the cost of adapting their existing product/service for DoD use, the profitability compared to the civilian market, the costs of the red tape and the public relations risks. Any extra work they have to do that is linked to the security environment may still have complementarities for civil work, or be covered by DoD expenditures. A reliable and steady flow of income from defence contracts and support for R&D may be seen as helpful for maintaining and developing their position in the civil market. With the DoD making every effort to involve them, the risk of the unknown, in entering a market they have little experience of, is reduced. It is really not surprising that the tech companies are keen to be involved in the defence sector.

What is unclear is how dependent they will become on defence orders and how much they will become part of the defence industrial base and take on the characteristics of the traditional arms firms. If they remain focussed on the expanding civil markets and the DoD orders remain a small part of their overall work, the answer is probably not much. If they become increasingly dependent on DoD orders, the answer is quite a lot. Then they are likely to start to become more active members of the MIC, engaging more with the military and DoD and with a vested interest in high and increasing military spending. If the strategy developed by the NSCAI is adopted and implemented, however, government will invest heavily in R&D in AI and other new and emerging technologies and may count on technological 'spin-in' from the commercial to the military market. Big Tech may then no longer be so interested in specific defence contracts.

What is interesting is how the tech companies seem to have already mastered the activities that are needed to operate in the MIC, which, combined with the changes being made by the DoD to encourage their involvement, puts them in a very powerful and potentially profitable position. Evidence of questionable behaviour in the JEDI contracts, comes from investigative journalists and the submissions in the contract appeal processes. It suggests rather cosy relations between the tech company directors and senior DoD staff, questionable lobbying activities and individuals moving between the tech companies and the Pentagon. Attempts to accommodate the tech firms have led to some procedures and rules not being followed. A DoD official who questioned the cosy relationship between the Pentagon and Bezos and Schmidt as being in conflict with DoD procurement rules was moved from the Defense Innovation Board

[119] 'Amazon Web Services makes nearly 67% of Amazon's operating profit in blockbuster quarter', GeekWire.com, 30 Jan. 2020, https://www.geekwire.com/2020/amazon-web-services-makes-nearly-67-amazons-operating-profit-blockbuster-quarter/

in 2017 and filed a grievance which was denied. Other concerns have centred on the DoD workers who have previously worked for Amazon and then returned to the private sector[120]. This all suggests that the tech firms are learning how to operate within the state and just within the law rather fast.[121]

There is, of course, the issue of how their employees will respond to involvement in the MIC and as the objections of employees at Google has shown, increased involvement with the DoD will not be without opposition. Certainly, the companies vary in their engagement with military business. Of the Big Five (FAMAG:FB, Amazon, Microsoft, Apple, Google, Facebook and Apple do not seem to be much involved, while Amazon, Google and Microsoft seem to be building up their engagement. There are also the other established high tech contractors, such as Oracle and IBM, who are looking to build up their contracts. It is possible at least initially, that the staff of some of the commercial tech firms may feel unhappy at a growing dependence on the DoD and that the increasing involvement in defence contracts will lead to the loss of staff. If these are staff that have generated the innovative nature of the firms, this could be damaging.

Traditional established defence contractors have not taken these developments lying down and they remain dominant in areas that the new tech companies are not involved in, the 'hard' side of weapons systems, infrastructure and support services. Interestingly, a contract for a $7.6 billion Defense Enterprise Office Solution (DEOS) project, which was expected to be won by Microsoft, was actually awarded to an established defense prime General Dynamics, in December 2019 (albeit through its recently acquired IT services company, CSRA). [122] This might suggest a reassertion of the established defence firms. However, by June 2020 the DoD was obliged to make a reassessment of the bidding process after protest from a competing bidder [123]. The protests have made accusations of irregularities in procedures.

There are three possible scenarios, cooperation, acquisition and competition. It will be interesting to watch this play out and see whether the dominance of the top defence contractors is halted, or whether they manage the processes at work. Cooperation would mean the very different cultures of the companies coming together. However, it is not clear this would be wanted by either side, as the different cultures may well come into conflict. As argued before, acquisition of the new tech companies by the established defence contractors is unlikely, as the big ones are too large. Taking over smaller companies to gain capabilities and technologies, as they have done in the past, is being tried by some of them, but is unlikely to work in the present situation. Again, the different cultures involved make it unlikely as smaller tech companies are likely to be swamped by the culture of the acquirer and may well lose the characteristics and staff that made them successful. In the similar dynamic of the 1980's computing industry it was common for acquisitions of small innovative companies by larger companies to lead to this. In some case the acquisition was only to get the technology and prevent it reaching the market in competition with the acquirers' own product/solution. Competition will not

[120] Though this may be just a feature of the US political system in general rather than specific to defence
[121] See the investigation by ProPublica: How Amazon and Silicon Valley Seduced the Pentagon — ProPublica https://www.propublica.org/article/how-amazon-and-silicon-valley...
[122] 'Analysts: Pentagon's multibillion-dollar DEOS contract is guaranteed for Microsoft', NextGov.com, 28 Mar. 2019, https://www.nextgov.com/it-modernization/2019/03/analysts-pentagons-multibillion-dollar-deos-contract-guaranteed-microsoft/155901/; and 'General Dynamics wins huge military cloud contract', Toolbox.com, 13 Dec. 2019. https://it.toolbox.com/article/general-dynamics-unit-wins-huge-military-cloud-contract .
[123] See details above in Section 4

necessarily mean direct confrontation if the companies simply stick to their market niches (Dunne et. al., 2020).

It is clear that the changes taking place are influencing state industry relations, with the involvement of the new tech company staff in advisory roles for the DoD and CIA leading to increased influence and revolving door opportunities issues. The questions are first, how far is the DoD willing and able to go in reforming arms procurement rules and processes to access new and innovative technologies developed by commercial technology companies. Second, whether or not such reforms will apply more broadly to defence contracting. As cloud computing and the use of AI, machine learning, automation, etc. becomes more important in the defence sector, so will the extensive security concerns. Civil firms are already dealing with such cybersecurity issues, but the requirements of the military are likely to differ and some of the defence companies are already active (Boulanin, 2013). It is looking likely that the resources assigned to cloud, IT, communications, remote sensing, AI and automation will grow and be dominated by new players. It might be the case that the established contractors give up on these contracts and focus on legacy systems and the development of autonomous and semi-autonomous weapons. Though they may also be providing the final products, even if not the underlying technology. It is also possible that now that the tech companies have seen what is available and become familiar with the DoD, they may even consider it worthwhile diversifying to the mainstream defence contracts and taking on the defence primes directly, though this is unlikely in the core defence areas. This raises the question as to how engagement of the US tech companies with the defence sector will change them. It is worth remembering that some of the defence majors would once have been considered dynamic companies at the cutting edge of technology, dominating fast moving civil technology markets.

6. Conclusions

This paper has considered the changes taking place in the DIB and MIC in the US, with the increased involvement of commercial technology companies. Context was provided by considering the developments that had taken place in the DIB since the end of the Cold War, identifying earlier technology changes and how the industry and state engaged with them. New developments in technologies, providing the foundations for the so called Revolution in Military Affairs, as well as the internationalisation of production and supply chains, the growth in the use of civil components, and the significant expansion of the military services area, all had significant impacts on the size and structure of the arms industry. Still, aall of them left in place a relatively stable DIB and maintained barriers to entry. The present developments, with a potentially high involvement of commercial tech companies, may have a more significant impact on the DIB and the MIC.

There has been a marked change in DoD's approach to military technology and a recognition of the need for reforming procurement to involve the civil tech firms. What changed was the recognition of the need for the technologies that had been developed in the dynamic civil markets that were well in advance of what the established defence companies could provide in AI, machine learning, automation, etc. The Big Tech companies have for some time spent far more than the DoD on R&D on these types of advanced technologies. Another difference to the past is the large size of some of the entering commercial tech companies, which generates challenges for the DoD to attract them to defence business. There was also an acceptance that the DoD and the military needed to develop their administrative structures to embrace the developments in cloud computing. The resulting JEDI project for a DoD cloud architecture system is the largest, most transformational of the DoD new technology projects, and is also of direct relevance for warfighting. It led to a controversial bidding process and led to some of the large civil tech companies fighting against each other for the contract.

While the JEDI project attracted bids from several of the large commercial tech companies, it is difficult to foresee how important defence contracts will be for the tech companies, given their large commercial markets. What is also difficult to foresee is the reaction of the established defence companies. While the arms market is undergoing important changes, it is still the case that a lot of money will continue to go on usual defence projects and weapon systems, so business will remain for the established firms. It is likely that the cloud, AI, machine learning and automation part of the budget will increase considerably, so the question is what the response of the established firms will be. A significant increase in cyber conflict could also further change the allocation of the budget. It might be the case that the established contractors give up on these contracts and focus on legacy systems and the development of autonomous and semi-autonomous weapons. It is also possible that the tech companies will consider it worthwhile diversifying to the mainstream defence contracts.

At present it is difficult to predict what is likely to happen or how this will affect the DIB. The established defence producers may fight back, both groups may stick to their specialisms, mergers may take place, or the new guys on the block may come to dominate defence production. Under the Trump administration the growth in the defence budget and support for exports reduced pressure on the established firms, but that may well change in the future. In terms of MIC dynamics, the recognition by the DoD of the need to access not only technologies from the commercial companies but also their expertise and advice has resulted in the appointment of leading figures from commercial tech to vital roles in DoD advisory boards and recruitment of tech company staff in arms procurement. What is striking is the speed with

which the larger tech companies have embraced the non standard methods of working within the MIC, with behind the scenes activity, intensive lobbying and movement of staff between the tech companies and the DoD. Interestingly, the 'revolving door' between the DoD seems to have gone from being seen as a concern, reflecting cronyism in the MIC, to a useful way of engaging the tech companies into the procurement systems, so it is no surprise that established arms firms and some DoD officials are calling foul.

Clearly, developments in the US are likely to be precursors of change in the international arms industry, but at present it is still unclear what they will be. It is likely that a similar kind of engagement with civil technology firms will occur, or is already occurring, in other countries, since the impact of the civil-military technology gap is present in other military establishments too and since their need to access commercial technologies will be similar. For many the engagement is with the US tech firms, especially if they are winning US defence contracts.

There will be some further competition, particularly from China, South Korea, Taiwan and some European countries, but it is not clear how this will develop. There are some interesting dynamics and the Trump administration's anti-China policies and the Huawei 5G debacle may be suggestive. Ericson and Nokia provide alternatives, but it is unclear how this will work out. Europe has no companies the size of the US new tech ones, but they do have capabilities.

It does look as though the international arms industry might well be at a crossroad, but it is unclear which path it will take. Further research is urgently needed to investigate the ongoing developments in the US as well as in other parts of the international arms industry.

References

Adams, Gordon, The Iron Triangle: The Politics of Defense Contracting, New York, Council on Economic Priorities, 1981.

Albertson, Dean (ed.), Eisenhower as President, New York, Hill and Wang, 1963.

Amara, J and R Franck (2020) The United States and its defence industries. Ch 2 in Keith Hartley and Jean Belin (eds) (2019) The Economics of the Global Defence Industry. Routledge, Abingdon, pp 7-34.

Bitzinger, R (ed) (2009) The Modern Defense Industry: Political, Economic and Technological Issues, Praeger Publishers, Westport, pp13-37. ISBN 978-0-275-99475-4.

Bonvillian, William Boone, Van Atta, Richard and Windham, Patrick (eds) 'The DARPA Model for Transformative Technologies: Perspectives on the U.S. Defense Advanced Research Projects Agency'. Open Book Publishers. 2019. http://library.oapen.org/handle/20.500.12657/23446

Boulanin, Vincent (2013). 'Cybersecurity and the arms industry', SIPRI Yearbook 2013, Oxford: Oxford University Press, 2013, section II, chapter 4, pp218-226.

Boulanin, Vincent and Maaike Verbruggen, 'Mapping the development of autonomy in weapons', SIPRI Report, Nov. 2017.

Briody, Dan 'The Halliburton Agenda' New Jersey, John Wiley, 2004.

Brzoska, Michael (2006) Trends in Global Military and Civilian Research and Development (R&D) and their Changing Interface, Mimeo, Munich.

Brzoska, Michael & Peter Lock (eds), Restructuring of Arms Production in Western Europe, Oxford, Oxford University Press, 1992.

Chapman, Gary & Yudken, Joel, Briefing Book on the Military-Industrial Complex, Washington DC, Council for a Livable World Education Fund, December 1992.

Dunne, J Paul, Elisabeth Sköns and Nan Tian, 'The changing economics of global arms production', PRISM, University of Cape Town, 2020.

Dunne, J Paul, Elisabeth Sköns and Nan Tian, Arms Production, Economics of', in Kurz, L (ed), Encyclopedia of Violence, Peace and Conflict, Forthcoming, 2020.

Dunne, J Paul (1995) "The Defence Industrial Base", Chapter 14 in Keith Hartley and Todd Sandler (eds) (1995) "Handbook in Defense Economics", Elsevier, pp 592-623.

Dunne, J Paul and Elisabeth Sköns (2010)"Military Industrial Complex". Chapter 20 in Tan, Andrew (ed) (2010) The Global Arms Trade: A Handbook. Europa / Routledge (London), pp 281-292. ISBN 978-1-85743-497-2.

Dunne, J Paul & Surry, Eamon, 'Arms Production', in SIPRI Yearbook 2006: Armaments, Disarmament and International Security, Oxford, Oxford University Press, 2006, pp 387-418.

Dunne, J Paul, Guy Lamb and Efi Nikolaidou "South Africa and its defence industry". Chapter in Keith Hartley and Jean Belin (eds) (2019) The Economics of the Global Defence Industry. Routledge, Abingdon, pp 547-570. PRISM working paper 2019-3 version here .

Dunne, J. Paul & Gordon Macdonald, 'Procurement in the Post Cold War World: A Case Study of the UK', in Claude Serfati (ed), The Future of European Arms Production, Cost A10 Action, Brussels, European Community Office for Official Publications, 2002.

Dunne, Paul "The Making of Arms in South Africa", Economics of Peace and Security Journal, Volume1, No. 1, January, 2006a. http://www.epsjournal.org.uk/pdfs/eps_v1n1_dunne.pdf

Dunne, J. Paul, Maria Garcia-Alonso, Paul Levine and Ron Smith "Determining the Defence Industrial Base." Defence and Peace Economics, 2007, Vol. 18, Issue 3, pp. 199-221, ISSN 1024 2694.

Dunne, J. Paul, Maria Garcia-Alonso, Paul Levine and Ron Smith "The Evolution of the International Arms Industries". Chapter 5 in Wolfram Elsner (ed) (2007) Arms, War, and Terrorism in the Global Economy Today -Economic Analyses and Civilian Alternatives. Transaction Publishers, New Brunswick (NJ, US) and LIT, Zurich, pp 97-120. ISBN 3-8258-0045-8.

Dunne, J. Paul (2009) "Developments in the Global Arms Industry from the End of the Cold War to the mid-2000s" Chapter 2 in Bitzinger, R (ed) (2009) The Modern Defense Industry: Political, Economic and Technological Issues, Praeger Publishers, Westport, pp13-37. ISBN 978-0-275-99475-4.

Eisenhower, Dwight, D. 'Farewell Radio and Television Address to the American People, January 17, 1961', Public Papers of the President of the United States, Dwight D. Eisenhower, 1960-61, Washington, D.C., 1961, pp. 1035-1040. Reproduced in Pursell, Carroll W. (ed.), The Military-Industrial Complex in Theory and Fact, New York, Harper & Row, 1972, pp. 204-208.

Gold, David, 'US military expenditure and the 2001 Quadrennial Defense Review', in SIPRI Yearbook 2002: Armaments, Disarmament and International security, Oxford, Oxford University Press, 2002, appendix 6E, pp. 309–322.

Government Accountability Office (GAO), Global War in Terrorism: Reported Obligations for the Department of Defense, GAO-08-1128R, Washington DC, 15 Sep. 2008.

Hartley, Keith and Jean Belin (eds), The Economics of the Global Defence Industry. Routledge, Abingdon, 2019.

Higgs, Robert (ed.), Arms Politics and the Economy: Historical and Contemporary Perspectives, The Independent Institute, New York, Holmes and Meier, 1990.

Kaldor, Mary, The Baroque Arsenal, Abacus Books, 1981.

Markusen, Ann R. & Sean S. Costigan (eds), Arming the Future: A Defense Industry for the 21st Century, New York, Council on Foreign Relations Press, 1999.

Melman, Seymour, The Permanent War Economy: American Capitalism in Decline, New York, Simon and Schuster, 1985.

Pages, Erik, 'Defense mergers: weapon cost, innovation, and international arms industry cooperation', in Markusen, Ann R. & Sean S. Costigan (eds), Arming the Future, New York, Council on Foreign Relations Press, 1999, ch. 7.

Perlo-Freeman, Sam & Sköns, Elisabeth, The Private Military Services Industry, SIPRI Insights on Peace & Security, No. 1, September 2008.

Perlo-Freeman, Sam, et al., 'Military expenditure', in SIPRI Yearbook 2009: Armaments, Disarmament and International Security, Oxford, OUP, 2009, pp. 185-189.

Raska, Michael (2020): 'The sixth RMA wave: Disruption in Military Affairs?', Journal of Strategic Studies, DOI: 10.1080/01402390.2020.1848818

Schwarz, Jordan A., 'Baruch, the New Deal and the origins of the military industrial complex', in Higgs, Robert (ed.), Arms, Politics and the Economy: Historical and Contemporary Perspectives, New York, Holmes and Meier, 1990.

Singer, Peter W., Corporate Warriors: The Rise of the Privatized Military Industry, Cornell Studies in Security Affairs, Ithaca, NY, Cornell University Press, 2003.

SIPRI Arms Transfers Database, accessible online at < http://www.sipri.org/contents/armstrad>.

SIPRI Yearbook: Armaments, Disarmament and International Security, Stockholm International Peace Research Institute, Oxford, Oxford University Press, various years.

Sköns, Elisabeth and Sam Perlo-Freeman, 'The United States' military spending and the 2011 budget crisis', in SIPRI Yearbook 2012, Oxford, OUP 2012, chapter 4, section III, pp162-166.

Sköns, Elisabeth, 'The US Defence Industry after the Cold War', chapter 17 in Tan, Andrew (ed), The Global Arms Trade: A Handbook, London, Routledge, 2010.

Sköns, Elisabeth, 'Omstruktureringen av vesteuropeisk forsvarsindustri: markedskrafternas logikk' ['Restructuring of the West European defence industry: the logic of market forces'], in Matlary, Janne Haaland & Osterud, Oyvind (eds), Mot et avnasjonalisert forsvar? [Towards a denationalized defence?], Oslo, Abstrakt Forlag, 2005.

Sköns, Elisabeth et al., 'Military expenditure', in SIPRI Yearbook 2004: Armaments, Disarmament and International Security, Oxford, OUP, 2004, pp 305-343.

Sköns, Elisabeth and Hannes Baumann, 'Arms production', in SIPRI Yearbook 2003: Armaments, Disarmament and International Security, Oxford, OUP, 2003, pp. 377-382.

Sköns, Elisabeth and Herbert Wulf, 'The internationalization of the arms industry', The Annals of the American Academy of Political and Social Science, vol. 535, no. 1 (Sep. 1994), pp. 43-57.

Slater, J. & T. Nardin, 'The concept of the military industrial complex', in Rosen, Steven (ed.), Testing The Theory Of The Military Industrial Complex. Lexington, Mass., Lexington Books, 1973, pp. 27-60.

Smith, Ron, Military Economics: The Interaction of Power and Money, Basingstoke, Palgrave Macmillan, 2009.

Tian, Nan et al., 'Global developments in military expenditure', in SIPRI Yearbook 2018, Oxford, OUP, 2018, chapter 4, section 1.

US Department of Defense (2018a), Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, Washington DC, Dec. 2018, available at: https://www.defense.gov/Explore/Spotlight/National-Defense-Strategy/

US Department of Defense (2018b), 'Summary of the 2018 Department of Defense Artificial Intelligence Strategy', Washington DC, 2018, available at https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

US National Security Commission on Artificial Intelligence, Final Report, March 2021, https://www.nscai.gov/2021-final-report/

Wulf, Herbert, Internationalizing and Privatizing War and Peace, Houndmills, Palgrave Macmillan, 2005.