New technology and the U.S. military industrial complex

J Paul Dunne and Elisabeth Sköns

J Paul Dunne is Emeritus Professor of Economics at PRISM, University of Cape Town and may best be reached at John.Dunne@uct.ac.za. Elisabeth Sköns is associate senior fellow at the Stockholm International Peace Research Institute (SIPRI) and may best be reached at eskons@sipri.org.

Abstract

This article considers what could be a fundamental development in the defense industrial base (DIB) in the U.S., namely the increased involvement of commercial technology companies in military-related business. 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. 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).

Since the mid-2010s, there have been developments in defense policy that have aimed to increase the engagement of commercial technology companies in military-related activities. This represents an important 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.

This article considers the changes that have been taking place and what they might mean for the future, focusing on developments in the U.S.—recognizing that these are often the precursors of change in the international arms industry and that most major commercial technology companies are also American. It asks whether recent developments in defense policy and arms acquisitions mean that the arms industry is undergoing another phase of structural and relational change. 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. Dunne and Sköns (2021) provide a more extensive set of references and more detail.

The next section provides background and context, outlining the main characteristics of the DIB and MIC from Cold War to post-Cold War developments. There is then a consideration of the changing approaches to military technology and the arms procurement system and the drivers behind these changes. There follows a further consideration of the new roles of the commercial technology industry in the military sector, the possible responses of the traditional defense contractors, and their implications. Finally, some conclusions are presented.

Development of the DIB/MIC

During the Cold War, the defense industry took on a particular structure that continues to influence developments now. The national government was the main customer, 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 amongst contractors, the procurement executive, and the military—most notable is the "revolving door", in which military and civil servants move to defense contractors they had dealings with and staff from defense contractors move into the bureaucracy. These characteristics tended to favor those firms who specialize in defense 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. Defense companies became experts at getting contracts out of government—these skills, along with the structure of the market, meant that there were both barriers to entry and barriers to exit.

The monopsonistic structure of the defense market, and the structures and relationships around it, led to remarkable stability in terms of its composition of near-monopoly main contractors during the Cold War. This millennium, however, has seen accelerating reliance on communication and control technologies which demand changing approaches to military technology and the arms procurement system. Vital new technologies lie with "Big Tech" companies in the commercial sector rather than with the traditional arms companies and are too large to be acquired by these traditional suppliers. The introduction of these tech companies has brought new ways of working but also has seen these companies adapt their commercial approaches to suit the nonstandard methods of working within the military industrial complex. It remains to be seen how this contested space will play out.

This led to the Cold War DIB showing remarkable stability in terms of its composition of main contractors. Monopsony in the defense market also helped to create near-monopolies for certain companies—particularly in smaller countries. Outside of the U.S., 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. Politicians also supported defense contacts that would benefit their voters. These developments then justified high levels of military spending and allowed inefficiencies to develop (Dunne and Sköns, 2010).

Post Cold War, 1990–99, the fall in military spending from its peak had a direct impact on the demand for the products of the DIB and the environment in which it operated—calling into question the ability of even the major countries to maintain a comprehensive domestic defense 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, turning into strong growth in 2001—particularly in the U.S., due to the massive spending made possible under the "global war on terror" label (justified primarily with the war in Afghanistan). Linked to the war on terrorism, there was also an explicit shift from a threat-based strategy to a capability-based strategy. Allowing for both continued investment in legacy systems and a transformation of military affairs, this shift in strategy allowed for the massive increase in U.S. military spending during the first decade of the new millennium

(Sköns and Perlo-Freeman, 2012).

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-centered 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 emphasize the way that improvements in information technology, precision targeting, and smart munitions created the possibility of a new form of warfare, network-centered warfare. It also changed the nature of military technology, with increased importance of software and ICT (information and communication technology) 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).

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 internationalization. The end of the Cold War did not bring about the expected diversification of the defense industry to civil products. Instead, there was a rapid process of ownership concentration through mergers and acquisitions. 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.[1] Subcontracting became increasingly important, increasing links with the civil sector and bringing new types of companies, particularly from the electronics and IT sectors, into the defense industrial base (Dunne et. al., 2007).

Another important factor was the internationalization of arms production in the post-Cold War period. This has taken two forms, the internationalization of ownership and the internationalization of supply chains. (Dunne, 2006). 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 U.S. (Sköns, 2010). New faces were introduced with 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 defense ministries to private companies and was expanded greatly during the war in Iraq (Perlo-Freeman and Sköns 2007; Wulf, 2005)

These developments all led to a defense industrial base that was looking rather different to the one inherited from the Cold War. In the U.S. 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.

In the early 2010s, 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 U.S. national security and defense strategy was commissioned. The Defense Strategic Guidance[2] identified a number of primary missions that required increased spending. These were counterterrorism and irregular warfare; deterrence and defense; power

1 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/.
2 U.S. Department of Defense (2012a).

projection capabilities in the face of asymmetric capabilities; and advanced and effective operational capabilities in cyberspace and space. In contrast, it included cuts in conventional ground forces and some major systems designed for the cold war, the so-called "legacy" systems.[3] In this environment of financial constraints and wartime transition, in November 2014, the U.S. Department of Defense (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". 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."[4,5] 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 U.S. military supremacy into the 2030s. It had 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.[6]

New tech and the U.S. Department of Defense

In 2015 Ashton Carter began his term as Secretary of Defense and was instrumental in developing new policy.[7] He had links with Silicon Valley and recognized the DoD would need to change to cooperate. He initiated personnel reforms to make it easier for DoD to bring in needed expertise; schemes to protect the intellectual property rights of commercial partners; 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 links with leading edge technologies from the tech start-ups.[8] Its leadership consisted of people with both military or DoD experience and Silicon Valley. In 2016, DIUx launched the Commercial Solutions Opening (CSO) process to open up and streamline the arms procurement system for innovative commercial technologies. Also in 2016, the Defense Innovation Board was set up 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), former CEO and executive chairman of Google and its parent Alphabet (2001–2017) and included other civil tech companies' leaders. There are a number of stories about these interactions. For example, during 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 center 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 USD 17m subcontract to provide image recognition software to identify

3 U.S. Department of Defense, (2012b).
4 "The Defense Innovation Initiative", Memorandum of the Secretary of Defense, U.S. Department of Defense, 2014. Available at: https://foreignpolicy.com/2020/10/23/semiconductors-china-united-states-defense-dependency/.
5 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 U.S. 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 (Ellman *et al*, 2016; 2017).
6 See the website of the Defense Innovation Initiative; Defense Innovation Marketplace: Connecting Industry and the Department of Defense, https://foreignpolicy.com/2020/10/23/semiconductors-china-united-states-defense-dependency/.
7 Much of the thinking behind the policy can be attributed to Bob Work, U.S. 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", U.S. DoD, Newsroom, 28 Apr. 2016,
https://www.defense.gov/Newsroom/Speeches/Speech/Article/753482/remarks-by-d%20eputy-secretary-work-on-third-offset-strategy/.
8 For a detailed account of the purpose, challenges and tasks of the Defense Innovation Unit, see Hummel and Schiller (2016).

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

drone targets. 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. 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 U.S. 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 (U.S. DoD, 2018a; U.S. DoD, 2018b). In 2018, DIUx was made permanent, expanded and renamed DIU, with contract awarding powers. In September 2017, a DoD memo had outlined a strategy to accelerate the DoD's adoption of cloud computing technologies, which it argued was critical to maintaining the U.S. military's technological advantage. [9] 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.

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.[10] Then in 2019, the National Security Commission on Artificial Intelligence (NSCAI) was set up to advise on the development of AI, machine learning and associated technologies[11]. In its final report in 2021 the main recommendations consisted of four pillars of action: leadership (by the government), with the creation of a Technology Competitiveness Council chaired by the Vice President; talent, proposing a new Digital Service Academy and civilian National Reserve to grow tech talent; hardware, with emphasis on supply chain resilience and security and federal investment to revitalize domestic microchip fabrication[12]; innovation investment, the establishment of a national AI research infrastructure and more funding and govt partnering with U.S. companies.[13].

These developments really do represent a change in attitudes. 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 defense industrial base and bring in the major commercial tech companies and entrepreneurs. This has left the established defense 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.

Detailed information on DoD activities with high tech companies is not available, but a dataset released in July 2020 by Tech Inquiry, a non-profit focusing on technology accountability, provides an extremely valuable source. It shows the relations to be greater than was thought. Silicon Valley companies were found to have thousands of previously unreported subcontracts with the U.S. military contractors, U.S. military, and federal law enforcement agencies. Big Tech companies such as Google, Amazon and Microsoft secured more than 5,000 agreements with agencies within the DoD. 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

9 "Accelerating Enterprise Cloud Adoption", Memorandum of the Deputy Secretary of Defense, 13 Sep. 2017. Published at NextGov.com, 9 May 2018. http://www.documentcloud.org/documents/4059163-DoD-Memo-Accelerating-Enterprise-Cloud-Adoption.html.
10 "About the JAIC", at the JAIC home page, https://www.ai.mil/about.html, visited 20 Sept 2020.
11 Final Report, National Security Commission on Artificial Intelligence, March 2021, available at https://www.nscai.gov/2021-final-report/.
12 U.S. NSCAI (2021) p. 3.
13 "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.

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

contracting" while smaller cutting-edge-tech firms lag behind.[14]

Some of the issues involved in the tech companies becoming involved with the DoD were illustrated in one of the early cases, Google's acquisition in December 2013 of Boston Dynamics, funded by DARPA and DoD to develop robots for military use.[15] 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[16]. 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.[17] 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.[18] Following a staff petition, Google decided to end its collaboration when the contract was up for renewal in March 2019.[19] 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).

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. The existence of reliable external cloud operators in the civil sector has become very common, as firms and organizations saw the benefits of outsourcing a big part of data management and storage. Cloud computing is of growing importance to both the civil and state sectors. 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 market consists of six main segments. First, infrastructure as a service (IaaS), the most advanced which develops the architectures. 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. Over time, the service provision has developed, with another three segments:

14 "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/.

15 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.

16 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/.

17 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/.

18 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/.

19 "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).

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

Business Process as a service (BPaaS), Cloud management and security services, and Desktop as a service (DaaS).[20] 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 defense 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), is the dynamic segment that is most relevant for the DoD. Amazon (AWS) has led the market since it began to offer IaaS in 2008. The 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. Amazon remains the market leader, with 45% of the global market in 2019. [21]

While the DoD has the same kind of needs as the commercial users, when moving their activities into cloud processes 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, it 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. [22] This is likely to make security concerns more onerous than in civil uses. That said, the cyber-attacks on the 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 organizing cyber defenses for the civil sector. Having recognized the potential importance of cloud services, the DoD also recognized the need to engage with the tech companies.

The first large DoD cloud initiative was the JEDI (Joint Enterprise Defense Infrastructure) project, worth USD 10 bn over 10 years. Its aim was to develop a comprehensive cloud enterprise system for overall DoD activities. Although this contract was substantially smaller than the largest DoD contracts for traditional weapons systems, it was significant in offering a contract of this size to a company outside the group of established defense contractors. This, in turn, reflects how important cloud computing had become, with the growth of the internet, and how far the military sector was lagging behind civil technology, capacity, and capability. In the JEDI process, two of the Big Five tech companies in the US—Amazon and Microsoft—were the two main competitors throughout the bidding process (as was Google initially). There was also one other major tech company, Oracle, and one of the traditional defense 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, stating that it believed this work would conflict with its corporate principles and because it believed it might not hold all of the capabilities or necessary certifications.[23]

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 Amazon Web Services (AWS). It also had the strongest share of the U.S. cloud services market, had been authorized with the required

20 Gartner, Press release, 23 July 2020 (note above).
21 "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.
22 "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/.
23"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.

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

security certifications, had been working on a similar USD 600m contract providing cloud services since 2013 to the CIA, and was also working on other smaller U.S. 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 favored 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 own legal process. Amazon's objections were considered and the DoD requested some time to reconsider its decision. However, after several delays the DoD reaffirmed its decision to award the contract to Microsoft, which resulted in a renewed protest by Amazon. In July 2021, this outdrawn process led DoD to cancel JEDI altogether. Instead, a new project idea was announced, this time as a multi cloud project, the Joint Warfighter Cloud Capability (JWCC) program, which will involve more than one prime contractor[24].

New tech and the U.S. defense industrial base

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. Defense firms have strikingly lower R&D expenditures, but this reflects that much of their R&D will have been covered by the DoD (Dunne and Sköns, 2021)[25]. There have also 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. This had rapidly dropped off, by the early 2010s military R&D was a much smaller part of national R&D, with tech companies leading the way instead (Dunne *et al*., 2020). Military R&D had also declined as a share of total R&D due to major increases in civilian expenditure. Increasingly civilian R&D occurred in technology lines important for the production of military goods and there was a major shift toward the military use of technologies driven by civilian R&D, particularly in electronics. In contrast to the arms companies, the big tech companies invest a considerable share of their revenues in R&D, with four of the five spending more than 10 percent of their revenues on R&D[26]. 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[27].

Unlike in previous innovations, such as the RMA, the established defense 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

[24] https://www.cnbc.com/2021/07/06/pentagon-cancels-10-billion-jedi-cloud-contract.html.

[25] Defense 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.

26 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.

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

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

and powerful to acquire 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 defense 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 technology 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 defense companies to adapt their technologies to military use. That said, with the changes in technology, a large part of defense spending is likely to go to the areas that the new tech companies are in. They are winning contracts and these are potentially large. 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 defense 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 around 67 percent of operating profit by the end of 2019.[28] Amazon is a company used to dealing with complex logistics, large amounts of data, and 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 defense 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 defense 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 defense 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 defense sector.

What is unclear is how dependent they will become on defense orders and how much they will become part of the defense industrial base and take on the characteristics of the traditional arms firms. If they remain focused 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

[28] "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/.

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

high and increasing military spending. If the strategy developed by the NSCAI is adopted and implemented, however, government will invest heavily in R&D, 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 defense contracts.

Interestingly, the tech companies do seem to have already mastered the tactics, methods and behavior that are needed to operate in the MIC. This, 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 behavior in the JEDI contracts, comes from investigative journalists and the submissions in the contract appeal processes. It suggests rather cozy 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 cozy relationship between the Pentagon and Bezos (amazon CEO at the time) and Schmidt as being in conflict with DoD procurement rules was moved from the Defense Innovation Board in 2017 and filed a grievance which was denied. Other concerns have centered on the DoD workers who have previously worked for Amazon and then returned to the private sector[29]. This all suggests that the tech firms are learning how to operate within the state and just within the law rather fast.[30]

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:Facebook, 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 defense 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 defense 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 USD 7.6bn 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). [31] This might suggest a reassertion of the established defense firms. However, by June 2020 the DoD was obliged to make a reassessment of the bidding process after protest from a competing bidder. 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 defense 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 defense contractors is unlikely, as the big ones are too large.

29 Though this may be just a feature of the U.S. political system in general rather than specific to defense
30 See the investigation by ProPublica, Bandler *et al* (2019).
31 "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 .

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

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 less likely to work in the present situation. The different cultures involved could mean smaller tech companies are 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 this to happen. 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. Of course, competition will not necessarily mean direct confrontation if the companies simply stick to their market niches, but this seems unlikely (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 eventually apply more broadly to defense contracting. As cloud computing and the use of AI, machine learning, automation, etc. becomes more important in the defense 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 defense 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 defense contracts and taking on the defense primes directly, though this is unlikely in the core defense areas. This raises the question as to how engagement of the U.S. tech companies with the defense sector will change them. It is worth remembering that some of the defense majors would once have been considered dynamic companies at the cutting edge of technology, dominating fast moving civil technology markets.

Conclusion

This article has argued that there are important changes taking place in the DIB and MIC in the U.S., with the increased involvement of commercial technology companies. 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 defense companies could provide in AI, machine learning, automation, etc. The Big Tech companies have for some time spent far more than the DoD and the traditional defense companies 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 defense 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 JEDI call for a DoD cloud architecture system was the largest, most transformational of the DoD new technology projects, and was 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. When it was cancelled the DoD announced its replacement by a multi-cloud, multi-vendor contract (JWCC), to avoid the destructive and fierce competition among the large civilian tech companies.

While there is interest, it is difficult to foresee how important defense contracts will be for the tech companies, given their large commercial markets. What is also difficult to foresee is the reaction of the established defense companies. While the arms market is undergoing important changes, it is still the case that a lot of money will

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

continue to go on usual defense projects and weapon systems, so business will remain for the established firms. It is, however, 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 defense contracts.

At present it is difficult to predict what is likely to happen or how this will affect the DIB. The established defense 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 defense production. 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 the recruitment of tech company staff in arms procurement. What is striking is the speed with which the larger tech companies have embraced the nonstandard 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 U.S. 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 governments and companies, the engagement is with the U.S. tech firms, especially if they are winning U.S. defense 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 U.S. anti-China policies and the Huawei 5G debacle may be suggestive. Europe has no companies the size of the U.S. 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 U.S. as well as in other parts of the international arms industry.

Acknowledgements

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 on an earlier version, but the usual disclaimer applies.

References

Bandler, J., Tsui, A. and Burke, D., 2019. How Amazon and Silicon Valley seduced the Pentagon. *ProPublica*. https://www.propublica.org/article/how-amazon-and-silicon-valley-seduced-the-pentagon

Boulanin, V. and Verbruggen, M., 2017. "*Mapping the development of autonomy in weapons*", SIPRI Report, Nov.

Boulanin, V., 2013. Cybersecurity and the arms industry. SIPRI Yearbook 2013: Armaments, disarmament and international security (pp. 218–226).

Dunne, J.P., 1995. The defence industrial base, 399–430. 1995). Handbook of Defence Economics: Defense in a Globalized World, Amsterdam, Elsevier. https://doi.org/10.1016/S1574-0013(05)80016-X

Dunne, J.P., 2009. Developments in the Global Arms Industry from the End of the Cold War to the Mid-2000s. The Modern Defense Industry: Political, Economic and Technological Issues. Westport, CT: Praeger, pp.13-37.

Vol. 16, No. 2 (2021) | doi:10.15355/epsj.16.2.5

Dunne, J.P., Garcia-Alonso, M., Levine, P. and Smith, R., 2007. The evolution of the international arms industries. Arms, War, and Terrorism in the Global Economy Today, (13), pp.97-120.

Dunne, J. P. and Sköns, E., 2010. Military Industrial Complex. In *The Global Arms Trade: A Handbook* (pp. 281–292). Europa / Routledge (London). https://doi.org/10.4324/9780203851456-24

Dunne, J. P. and Sköns, E., 2021 New Technology and the Changing Military Industrial Complex, *PRISM Working Papers*, University of Cape Town. http://www.prism.uct.ac.za/prism/Working-Paper-Series

Dunne, J. P.,Sköns, E. and Tian, N., 2020 Arms Production, Economics of. In *Encyclopedia of Violence, Peace and Conflict*. Academic Press.

Ellman, J., Cohen, S., Hunter, A. and Johnson, K., 2017. Defense Acquisition Trends, 2016. Rowman & Littlefield. https://www.csis.org/analysis/defense-acquisition-trends-2016.

Hunter, A.P., McCormick, R., Ellman, J., Sanders, G., Johnson, K. and Coll, G., 2016. Defense acquisition trends, 2015. Center for Strategic & International Studies, Tech. Rep, p.118. https://www.csis.org/analysis/defense-acquisition-trends-2016.

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

Hummel, R.H. and Schiller, K., 2016 "*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.

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

Perlo-Freeman, S. and Sköns, E., 2008. The private military services industry. *SIPRI Insights on Peace and Security*, no. 2008/1, Sep. 2008.

Sköns, E. and Perlo-Freeman, S., 2012. The United States' military spending and the 2011 budget crisis. SIPRI Yearbook 2012: Armaments, Disarmament and International Security.

Sköns, E., 2010. The U.S. Defence Industry after the Cold War, *The Global Arms Trade: A Handbook*. London, Routledge.

Smith, Ron, 2009. *Military Economics: The Interaction of Power and Money*, Basingstoke, Palgrave Macmillan. https://doi.org/10.1057/9780230244672_2.

U.S. Department of Defense, 2012a. *The Defense Strategic Guidance*, Department of Defense: Washington, DC.

U.S. Department of Defense, 2012b. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Department of Defense: Washington, DC, Jan.

[U.S. DoD] U.S. 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. available at: https://www.defense.gov/Explore/Spotlight/National-Defense-Strategy/

[U.S. DoD] U.S. Department of Defense, 2018b. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, Department of Defense: Washington DC. available at: https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

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

Wulf, H., 2005. *Internationalizing and Privatizing War and Peace*. Houndmills, Palgrave Macmillan. https://doi.org/10.1057/9780230514812.