DARPA and the American Approach

Delivering National Scientific & Technological Advantage

William Schneider, Jr

Visiting Scholar at Policy Exchange

William Schneider, Jr

Delivering National Scientific & Technological Advantage:
Darpa and the American Approach

Transcript

Author Note

William Schneider, Jr is a Visiting Fellow at Policy Exchange and Senior Fellow at the Hudson Institute, Washington, DC, and Member, US DoD Defense Science Board. This is a transcript of a speech delivered to Policy Exchange on 30 January 2020. A video of the event can be found here.

1. Introduction

It is a trite, but nevertheless, true observation that 'necessity is the mother of invention'. For most nations, there are few domains of public investment that offer a more compelling necessity than national defense. Hence the process of the conversion of insights from the frontier of fundamental science into technologies that can, in turn create military capabilities has been a characteristic of nation-states for centuries. The wartime creation of the military applications of atomic energy and digital computers are well-known wartime scientific and engineering innovations whose civil applications have had profound applications to modern life.

In digging in a bit more deeply, it may be useful to consider how the technology of atomic energy and the digital computer evolved from their military to civil applications.

The transition of these technologies from military to civil applications illustrate Peter Thiel's observation concerning the government regulation of innovation. Thiel observed that government practice regulates atoms, while bits are unregulated. This point is not always and everywhere true, but it is a useful generalization that helps understand why IT based technologies enabled a rich environment for innovation compared to more highly regulated activities.

In 1953, President Eisenhower proposed "Atoms for Peace" as an approach to developing the civil applications of atomic energy. However, the civil applications of atomic energy were then and are now a government dominated and regulated activity in every major nation that applies atomic energy to civil applications. As a result, innovation is slow in part because the pace of regulatory activities is inconsistent with the private financing of its applications and the pace of the implementation of innovative applications of the technologies.

The evolution of digital computers differed. Following World War II, government-developed knowledge of digital computers (primarily in the UK and US) was widely shared with private industry; the rate of progress was and remains extraordinary.

Today, many new technologies that can be reduced to "information" (e.g. genomics, biology, telecommunications, etc.) can then be processed in the form of software and modern modeling and

simulation (M&S). Developmental application using M&S can diminish or in some cases, eliminate costly and time-consuming experiments, and contribute to the creation of technologies and their application that often grow at an exponential rate rather than in a linear fashion with which we are most familiar. The growth of the underlying technologies of autonomy are in many cases, growing at an exponential rate that is accelerating the development of fielding autonomous vehicles and the Internet of Things. Adapting to the rapid growth of many of the core technologies that enable modern civil and military capabilities has become among the most challenging characteristics of modern life.

These circumstances illustrate an important aspect of how the innovation process for national defense is being changed in fundamental ways. Historically the application of advanced technology for national defense purposes was undertaken in government arsenals, usually in secret for subsequent wartime application. The civil applications developed in these circumstances slowly "trickled down" to the civil sector. In the American setting, the Constitutional injunction to "maintain a Navy" but "raise an Army" left America unprepared the vast scale of global conflict that characterized the wars of the first half of the 20th century. This hard-won experience reinforced the importance of alliance relationships in US foreign policy, and to necessity of having an responsive S&T and industrial base in place before a conflict begins.

An expedient civilian defense-industrial infrastructure was created to respond to World War II US and alliance mobilization needs to support the war effort. A vast infrastructure was created to support the 16 million Americans served in the US armed forces. This underlying defense-industrial enterprise employed 24 million people in the US in World War II.

Through sharply reduced in size, the wartime "expedient" infrastructure became a permanent aspect of national defense as the Cold War settled in as a permanent feature of daily life following the end of Korean conflict in 1953. Nevertheless, the technologies that underpinned the Cold War cycles of modernization and recapitalization continued to develop in the US and later, within the alliance defense industrial base. The US and its allies began the process of integrating new technologies (advanced materials and manufacturing technologies, microelectronics, space operations, etc.) to create advanced military capabilities.

To broaden access to advanced technology, the DoD deregulated the foreign investment in the US defense sector in the 1980s that permitted ~ 200 international defense firms to participate directly in the US defense market. This participation in the US defense market included access to classified information and defense contracting rights equivalent to indigenous firms, and the ability to participate in the US Foreign Military Sales system.

The inexorable transition of national defense from an activity dominated by kinetic operations on a massive industrial scale evolved in the 1980s to a mixture of kinetic and non-kinetic operations. These capabilities were predominately created by the technologies of information. Recent US military history illustrates the scale, scope, and impact of these trends. In the multi-national *Operation Desert Storm/Shield* in 1991 to expel Iraq from Kuwait over a four-day period of day-night-all weather operations involved nearly 500 thousand US troops, a logistics support force 4000 contract personnel from 76 US and 22 foreign contractors, and a supply infrastructure of 360,000 military cargo containers.

Without attempting to engage the intense diplomatic and policy disputes surrounding the subsequent US and allied operations in Iraq (and elsewhere) little more than a decade later offers some useful insights. The military outcome of the major combat operations reflected the growing dominance of information on the battlefield, and its importance to the narrative about the path of innovation. In *Operation Iraqi Freedom*, 177 thousand coalition forces including 130,000 from the US (one-third of

their 1991 complement) conducted continuous day-night-all-weather combat operations throughout Iraq for 21 days to defeat Iraq's armed forces. Employing the technologies of information enabled combat operations with a with a significantly smaller troop complement than had previously been required.

This was possible because the technologies of information had a profound effect reducing the scale of operations needed to produce decisive military effects. Modern information-based technologies of intelligence, surveillance, and reconnaissance (ISR) diminished the "fog of war" to an extent that much smaller forces were needed to create a desired military effect without the need to retain large reserve forces in the theater of operations. In this context, 'bandwidth' (to collect, process, and disseminate tactically decisive information in a timely manner) effectively allowed the combatant commander to replace large reserve forces with the insights made possible by IT-enabled ISR.

The cumulative effect of the increasing role of information, and more generally, the importance of technologies developed outside of the defense sector has significantly reduced the financial burden of national defense. At the zenith of the Cold War (during the Cuban Missile Crisis in 1962), the nearly ten percent of the US GDP was devoted to national defense. Today that figure has declined by two-thirds, and despite the large increase in defense expenditure since 2017, national defense only absorbs 3% of the US GDP.

2. National defense in an age of inter-State conflict

The characteristics of modern warfare enabled by the growing role of information in the national defense function has made it increasingly difficult for the legal and diplomatic practices built around classic kinetic military operations to function effectively. Hostile acts can be undertaken invisibly and long before the first shot is fired. These pre-kinetic measures can vastly expand the scope, duration, and destructiveness of conflict. A few elements of warfare that are enabled by modern technology are illustrative.

a. The 'homeland' is no longer a sanctuary; the civil infrastructure that enables modern warfare is highly vulnerable and likely to be exploited

The modern practice of warfare – reinforced by international law – was focused on engagements between military forces of nation-States. The devastating experience in World War II resulting from the practice of targeting civilians and their infrastructure has regrettably been expanded in the 21st century. Information technology-enabled vulnerabilities in both the civil and military infrastructure provide new opportunities to engage an adversary. This can include attacks on the adversary's homeland to diminish the capacity of its defense industrial base to respond to operation needs as well as his ability to marshal and deploy military forces. Rather than being attacked last, the homeland in non-kinetic form likely to be attacked first by State adversaries.

The remarkable capabilities created by the incorporation of information technology in the modern civil infrastructure have also created extraordinary vulnerabilities. The 17 elements of the US critical infrastructure are jointly linked to the day-to-day operations of both civil society and the US defense

establishment. Their shared vulnerability unites them. Their prolonged loss would also catastrophic to both US security and its economy.[1]

The civil infrastructure is an indispensable element of the national capacity to mobilize and deploy resources for a conflict abroad. The US global deployment infrastructure is based on an expectation of a secure homeland. While some measures are now being taken to mitigate the exposure of key elements of the critical infrastructure, they are likely to be concentrated on the ability of the armed forces to mobilize, deploy, and sustain military operations.

b. Modern threats are increasingly built around very rapidly developing dual-use technologies challenging both the security and competitiveness of all industrial democracies, not only the US and the UK

China has institutionalized its aspirations for the development and exploitation of advanced technology, particularly dual use technologies with military and civil applications. Although public advocacy of the policy has been attenuated to mitigate trade friction, its "Made in China 2025" policy remains an organizing principle for State investment. Uniquely, China has integrated its investment strategy in these technologies with its policy of "civil-military fusion". This approach enables China to extract military applications from these technologies in parallel with its development of their civil applications. This contrasts with US practice using specialized defense entities (defense industry and the DoD R&D ecosystem) to develop defense applications of civil sector technology. US civil sector investment in dual use technologies typically far exceeds that of the defense sector as the defense sector is highly risk averse.
The defense sector tends not to exploit advanced civil sector technology until it is relatively mature. Chinese investment policy has concentrated resources in ten segments in conjunction with large-scale investment in scientific and engineering infrastructure to simultaneously develop the technologies for civil as well as military applications China seeks the early integration of civil technology into its defense sector.[2]

c. The domains of conflict are more numerous and complex in their interaction with kinetic military operations offering opportunities for the clandestine 'preparation of the battlefield' long before the outbreak of hostilities as well as throughout the period of conflict

The familiar domains of military power – land, sea, and air – continue to dominate the thinking of governments and citizens alike. However, since the end of the Cold War and the intense applications of the technologies of information, seven additional domains of conflict have been added including space in the physical domain, including cyber, the electromagnetic spectrum and information operations in the virtual domain, plus social, moral, and cognitive elements in the 'human' domains of warfare.

1 ***Presidential Policy Directive 21 Critical Infrastructure Security and Resilience*** (2013); https://www.cisa.gov/critical-infrastructure-sectors; and ***Executive Order 13636***; ***Improving Critical Infrastructure Cyber Security*** (2013); https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf

2 These segments are IT, robotics, green energy and vehicles, aerospace equipment, ocean engineering & high-tech ships, railway equipment, power equipment, materials, medicine and medical devices, and agricultural machinery. Elsa B. Kania, ***Made in China 2025 Explained***, February 1, 2019, *The Diplomat*, https://thediplomat.com/2019/02/made-in-china-2025-explained/. Lorand Laskai, ***Civil-Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies***, *Jamestown Foundation China Brief*, April 9, 2018; https://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/

Emerging technologies developed outside of the defense sector contribute significantly to the creation of military capabilities. These technologies are also most likely to have innovative civil applications.

DOMAINS OF WARFARE

Physical	Virtual	Human
Land	Cyber	Social
Sea	Electromagnetic Spectrum	Moral
Air	Information	Cognitive
Space		

Among the most significant military developments contributing to bringing the Cold War to a peaceful end was the DARPA-led development of what became known as the *Assault Breaker I.* This technology-enabled concept of operations was developed in the 1970s and '80s and was aimed at the core of Soviet military power in Europe. Soviet dominance of Europe was built upon its ability to reinforce its air and ground forces deployed in Central and Eastern Europe since 1945 with its echeloned reserve forces located in the Western Military Districts of the former USSR.

DARPA's *Assault Breaker I* concept integrated long-range airborne ground-surveillance radar with precision munitions to permit the delivery of precision strikes against the echeloned reinforcement of Soviet forces based in the Western Military districts of the USSR. This capability denied the Soviet forces their capacity to defeat NATO's conventional military force in Europe. The Soviet and Warsaw Pact recognition of this "ground-truth" created by technology-enable military capabilities contributed to the unraveling of the Warsaw Pact, and the collapse of Soviet military power and authority in Europe in 1989-91.

China's foreign policy aims have also evolved significantly since the end of the Cold War. China has expanded the geographic scope of its aspirations. They have grown from those of the Deng Xiaoping era (1978-92) where China sought to become the leading State in the East Asian region. China's emerging global aspirations to become the world's leading economic and military power by 2049 developed under President Xi were codified in the 19th Congress of the Communist Party of China in 2017. These developments increase the risk of conflicts of interest in the future.

Similarly, Russia's aspirations to modernize and become culturally and economically integrated with Europe following the collapse of the former Soviet Union were quickly abandoned following the end of the Yeltsin government. It was replaced by a Eurasia-focused kleptocratic leadership under Vladimir Putin in 1999. Russian policy regards the US as its main adversary; it initiated a large-scale program of the modernization of it strategic and sub-strategic forces in 2009 following its signing of the "Spirit of Prague Declaration and New START, and changed its doctrine of nuclear use in 2014 to include the limited use of nuclear weapons in a conventional conflict. Chinese and Russian military cooperation including joint exercises from the Baltic Sea to the South China Sea has become a regular feature of their military activities.

Chinese and Russian defense collaboration has been complemented by increasing diplomatic collaboration on a global basis aimed at undermining US alliance relations and leveraging Russia's Private Military Contractors to conduct military operations that the government denies.

Taken together, these developments led the US government to reduce the prominence of its counterterrorism focus without abandoning it and change its national security policy. In 2017,the US government promulgated a new national security strategy that emphasized the need to be "capable of deterring and defeating the full range of threats to the United States", including China and Russia as peer competitor States. This evolution of US policy has led to the development of the technology

base for *Assault Breaker II*. DARPA is now engaged in developing the key enabling technologies to support the policy objective.

3. Space: An opportunity for technology-enabled innovation

When Prime Minister Thatcher decided to withdraw from Britain's efforts to create its own space program in collaboration with the EU, a private sector entity emerged committed to space system development. The effort, led by the University of Surrey's highly regarded innovator in satellite system development, Professor Sir Martin Sweeting stepped in and became a leading developer of small satellites that met the needs of many users. He exploited the excess capacity that existed in the existing expendable launch vehicle market to gain access for his small satellites to space. Indeed, the way space system technology has subsequently evolved, the entire sector has moving rapidly toward deploying large numbers of small satellites rather than the 15-ton behemoths of the past. Over the next decade, telecommunications companies, internet operators, and other users are expected to launch ~ 40,000 satellites into orbit.

The emerging path of innovation in space offers new outlets for British science and technology. The "Billionaires Club" of extraordinarily successful entrepreneurs have incorporated the development of reusable space vehicles in their investment portfolio. This innovation enables a vast reduction in the cost of gaining access to space. When it was operational, the US Space Shuttle cost $54,000/kg to place a payload in space. A recent cost of a SpaceX mission to the International Space Station was $2,700/kg.

Moreover, the rapidity with which reusable systems can place payloads in orbit further reduces the cost of space access for military operations. For example, the US firm, SpaceX, led by the South African born entrepreneur, Elon Musk has recently built and launched 60 satellites for the US Air Force in four months. Using conventional expendable launch vehicles, such a task would have taken years to complete. The advantage for providing access to space is rapidly shifting away from the large-scale government-dominated space launch infrastructure to a privately-run reusable space launch vehicle-based system.

With access to space becoming commoditized, an opportunity emerges for British science and engineering expertise to concentrate on space missions, applications, and payloads for both civil and national defense applications to meet national needs. The ability to proliferate small space platforms – pioneered in Britain as a result of PM Thatcher's decision to abstain from participation in a European space venture – can now serve as the basis for the ability of Britain to include space ventures as part of its national innovation portfolio.

4. Institutional opportunities to facilitate innovation – a UK 'ARPA'

Perhaps the most vexing question for HMG is whether it will create an ARPA-like institution, and if it does, whether it can be organized in a manner that can create the sort of outcomes that have characterized the performance of its US counterpart. There is evidence of strong support for the creation of such an institution, but some of concepts for a UK 'ARPA' pose significant risks to the aspirations of its proponents. Several Departments of the US government as well as governments abroad have sought to replicate DARPA's success. Alas, these efforts are unblemished by success.

The US DARPA is a technology-based institution that is focused on creating new capabilities, not technologies for the Department of Defense. As several of DARPA's 22 former Directors have underscored, DARPA has had an enduring description of its technology-based mission:

> *Make pivotal investments in breakthrough technologies for national security, and through its investment to catalyze the development of new capabilities that give the Nation technology-based options for preventing – and creating – technological surprise.*

To achieve these aims, DARPA has a simple six-office structure that are not aligned by either technology or mission application. Instead are focused on creating military capabilities and are so described by DARPA. DARPA's publishes an annual strategy document that describes its activities for the year ahead.[3]

- **Biological Technologies Office:** DARPA's Biological Technologies Office develops capabilities that embrace the unique properties of biology—adaptation, replication, complexity—and applies those features to revolutionize how the United States defends the homeland and prepares and protects its Soldiers, Sailors, Airmen, and Marines. BTO is helping the Department of Defense to counter novel forms of bioterrorism, deploy innovative biological countermeasures to protect U.S. forces, and accelerate warfighter readiness and overmatch to confront adversary threats.

- **Defense Sciences Office:** DARPA's Defense Sciences Office (sometimes described as "DARPA's DARPA") identifies and pursues high-risk, high-payoff research initiatives across a broad spectrum of science and engineering disciplines and transforms them into important, new game-changing technologies for U.S. national security. Current DSO themes include frontiers in math, computation and design, limits of sensing and sensors, complex social systems, and anticipating surprise. DSO relies on the greater scientific research community to help identify and explore ideas that could potentially revolutionize the state-of-the-art.

- **Information Innovation Office:** Modern society depends on information and information depends on information systems. Timely, insightful, reliable, and relevant information is essential, particularly for national security. To ensure information advantage for the U.S. and its allies, the Information Innovation Office (I2O) sponsors basic and applied research in three thrust areas: Symbiosis, Analytics, and Cyber.

- **Microsystems Technology Office**: The Microsystems Technology Office's (MTO) core mission is to develop high-performance intelligent microsystems and next-generation components to ensure U.S. dominance in the areas of Command, Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance (C4ISR), Electronic Warfare (EW), and Directed Energy (DE). The effectiveness, survivability, and lethality of these systems depend critically on the microsystems contained inside.

- **Strategic Technology Office:** DARPA's Strategic Technology Office (STO) is focused on technologies that enable fighting as a network to increase military effectiveness, cost leverage, and adaptability.

[3] ***DARPA's 2019 Framework***; https://www.darpa.mil/attachments/DARPA-2019-framework.pdf

- **Tactical Technology Office:** The mission of DARPA/TTO is to provide or prevent strategic and tactical surprise with very high-payoff, high-risk development and demonstration of revolutionary new platforms in Ground Systems, Maritime (Surface and Undersea) Systems, Air Systems, and Space Systems.

The importance of a technology-enabled focus to create new capabilities is a decisive dimension of DARPA's writ, and separates it from other organizations – public and private – within the DoD's national defense R&D ecosystem. Other organizations such as the laboratories for each of the Military Departments apply an integrated suite of technologies relevant to the mission of their respective service – in many cases, developing service-specific applications of capabilities that have been demonstrated through a DARPA program.

DARPA's concentration on the creation of capabilities mitigates a technological vice that is often associated with organization structures that seek to create outcomes based on a top-down priority to create a specific outcome or outcomes in specific mission applications. This approach tends to create specific technology proponents who often develop a pre-disposition akin to the carpenter whose only tool is a hammer – in which case, every problem appears to be a nail.

Efforts to create DARPA-like entities have fallen prey to more traditional governmental bureaucratic objections and concerns; opposition to lateral entry into government service, authority-based processes to authorize the expenditure of appropriated funds, and layers of governmental supervision, etc.

The risks and difficulties associated with the creation of a UK ARPA to address its aspirations for the development of a culture of innovation in government-sponsored R&D need to be addressed. However, there is no need to make the initiative more difficult than necessary.

There are in fact existing bilateral arrangements already in place that, with a modest level of diplomatic ingenuity could be put to work to contribute to the government's ability to create a UK ARPA. There is a rich fabric of US-UK bilateral agreements and institutional arrangements relating to defense R&D going back to the wartime Quebec Conference in 1943. A bilateral Memorandum of Understanding was negotiated in 2000 that offers an extensive diplomatic basis for more extensive collaboration, both technically and institutionally.[4]

The scale of the US defense R&D ecosystem also offers opportunities for a UK ARPA to develop relationships with US institutions that do not have counterparts in the UK system, particularly Federally Funded Research & Development Centers (FFRDCs) of which the DoD has nearly 40 such institutions. The identification and development of collaborative opportunities for a UK ARPA is too large a subject to be effectively addressed here. Suffice to say, it would be constructive for the UK to consider ways in which it can build on the rich underpinnings already in place to facilitate leveraging bilateral collaboration to help make the UK ARPA successful.

A second existing institutional opportunity is the US-UK Defense Trade Cooperation Treaty. This Treaty is permissive of a very effective bilateral arrangement that can integrate defense R&D and defense trade. Alas, the implementing regulations inserted coincident with Senate ratification of the Treaty in 2010 made implementation of the Treaty's provisions infeasible.[5] Moreover, the UK is by far

[4] ***DEFENSE Research and Development Projects Memorandum of Understanding Between the UNITED STATES OF AMERICA and the UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND***; April, 2000; https://fas.org/sgp/othergov/us-uk-research.pdf

[5] ***United Kingdom / United States of America Defense Trade Cooperation Treaty***; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709579/UK-US-Defense-Trade-Cooperation-Treaty-V-1.1-May-

the largest and most successful direct investor in the US defense market providing a transatlantic presence for UK industry that might be a constructive element in HMG's development of a UK ARPA. The environment for defense R&D cooperation today is far better than was the case a decade ago as the US government seeks to improve the environment for defense-industrial and scientific cooperation with its closest allies, the UK and Australia.[6] Exploiting the provisions of this highly permissive treaty could contribute to the success of a UK ARPA.

A third though less institutionalized opportunity may exist for bilateral collaboration in joint studies of defense related R&D and its links to parallel or derived civil applications. An illustration of this opportunity is a joint study effort undertaken several years ago between the US *Defense Science Board* and its UK counterpart, the MoD *Defence Scientific Advisory Council* on defense-critical technologies.[7] This timely study effort examined five transformation technology areas critical to the defense needs of both nations. There are likely to be future opportunities to create similar joint study efforts with other defense-related institutions that can contribute to shaping both the form and content of a UK ARPA.

The establishment of a UK ARPA is a 'high-risk/high-payoff' opportunity. Understanding why it has proven so difficult in both the US as well as in an international context to replicate the US experience with ARPA/DARPA is crucial. Such an understanding can be as helpful to both HMG and the MoD in establishing the aims and infrastructure for the UK counterpart.

2018.pdf. The leadership of the Senate Foreign Relations Committee during the ratification were strongly opposed to the Treaty because of its potential to facilitate international arms sales which the Committee's two Chairman during the period of ratification (2007-10) opposed.

6 The recently published report (2018) of the President on the US defense industrial base endorsed the FY2017 National Defense Authorization Act, Section 881 provision that added the United Kingdom of Great Britain and Northern Ireland and Australia to the definition of the National Technology and Industrial Base. President Donald J. Trump, ***Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*** (2018), https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

7 ***Joint US Defense Science Board-UK Defence Scientific Advisory Council Task Force on Defense Critical Technologies*** (2006); https://dsb.cto.mil/reports/2000s/ADA446196.pdf