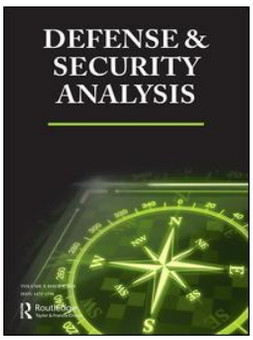

Defense & Security Analysis

ISSN: 1475-1798 (Print) 1475-1801 (Online) Journal homepage: https://www.tandfonline.com/loi/cdan20

United States defence contractors and the future of military operations

Charles W. Mahoney

To cite this article: Charles W. Mahoney (2020): United States defence contractors and the future of military operations, Defense & Security Analysis, DOI: 10.1080/14751798.2020.1750182

To link to this article: https://doi.org/10.1080/14751798.2020.1750182

Published online: 20 Apr 2020.

DEFENSE & SECURITY ANALYSIS
https://doi.org/10.1080/14751798.2020.1750182

Routledge
Taylor & Francis Group

United States defence contractors and the future of military operations

Charles W. Mahoney

Department of Political Science, California State University, Long Beach, CA, USA

ABSTRACT

The United States' global strategic outlook has shifted markedly since the end of major combat operations in Iraq and Afghanistan. As the United States' strategic posture shifts, the nature of military operations is simultaneously changing rapidly. Many analysts predict that cyber-operations, autonomous weapons systems, artificial intelligence, and clandestine special forces operations will be central features in future conflicts. Although often overlooked by scholars and policy analysts, defence contractors are integral to the development and implementation of these emerging categories of warfare. This inquiry examines the evolving nature of the American defence industry and the roles corporations play in current theatres of conflict. Surprisingly, rather than becoming less reliant on defence contractors after their much-maligned performance in the wars in Iraq and Afghanistan, American military and intelligence agencies have become more dependent on the private sector as technology becomes increasingly central to warfare.

KEYWORDS

Defense contractors; private military and security companies; Cyber operations; drones; outsourcing; United States

Introduction

The United States' global strategic outlook has shifted markedly since the conclusion of major combat operations in Iraq and Afghanistan.[1] The absence of a major terrorist incident on United States soil since the 9/11 attacks has caused the American defence community to de-prioritise the future threat posed by non-state extremist groups.[2] Although jihadist organisations operating in failing states still represent a concern for policy-makers, new challenges presented by great powers have regained a central position in the United States' long-term strategic planning.[3] Many foreign policy experts now view traditional state competitors including China and Russia as the primary security threats to American interests.[4] As the United States' strategic outlook shifts, the nature of both conventional and irregular conflict are also changing rapidly.[5] An ongoing revolution in military affairs promises to make Cyber-operations, autonomous weapons systems, artificial intelligence, and clandestine special forces operations central features in future conflicts.[6]

Amid this rapidly changing strategic and technological landscape, corporations in defence industry are preparing for a major role in future American military operations. Surprisingly, although defence contractors' record in the wars in Iraq and Afghanistan

CONTACT Charles W. Mahoney Charles.Mahoney@csulb.edu

was widely criticised for costing taxpayers an estimated $30 billion in overcharges and included documented instances of human rights violations—United States government spending on corporations in the defence industry has risen markedly in recent years.[7] Between 2000–2017, the Department of Defense's (DoD) fiscal obligations to contractors grew by 69 percent in inflation adjusted United States dollars, totalling $320 billion in 2017—accounting for 55 percent of DoD's budget.[8] American armed forces and intelligence agencies increasingly turn to corporations not only to develop new technologies and weapons systems, but also to provide the labour force required to pilot unmanned aerial vehicles, carry out Cyber-operations, conduct warzone intelligence analysis, and train foreign troops involved in civil conflicts.[9]

This inquiry evaluates the changing nature of the United States defence industry and assesses the emerging services corporations provide to American military and intelligence agencies. The central argument advanced is that United States defence contractors have learned from the corporate experience of Blackwater in Iraq and presently are wary of participating in activities that may involve them in direct, physical conflict with enemy forces. Thus, among major defence contractors, there is a growing aversion to supplying "protection services" in combat zones.[10] Furthermore, the United States' de-prioritisation of counter-insurgency operations has caused some corporations providing security services to experience significant financial decline. For example, Constellis—the company that formed from the merger of security providers Blackwater and Triple Canopy—recently defaulted on its credit obligations.[11] Despite a general retreat from security service provision, corporations operating in the United States defence industry still risk taking part in inherently governmental activities that could lead to the use of lethal force as they increasingly participate in offensive Cyber-operations, intelligence analysis resulting in drone strikes, and advisory roles in failing states.[12] More broadly, with over half the American defence budget spent on hardware and services provided by corporations, the United States' national security responsibilities have become outsourced to such an extent that a recent Congressional Research Report noted: "without contractor support, the United States would not be able to arm and field an effective fighting force."[13] As an essentially public/private hybrid—rather than the public institution it is perceived to be by the American people—the United States armed forces have a strong interest in promoting the financial stability and growth of the leading corporations in defence industry. After decades of consolidation, many defence contractors are today deeply embedded within the United States' security and economic architecture and are, for all intents and purposes, too big to fail.[14]

This article is organised into three parts. The first examines the current financial and technological landscape of the United States defence industry as it has undergone a major upheaval since the end of the major combat operations in Iraq and Afghanistan. The second section describes how defence contractors are currently supporting American military and intelligence missions around the globe by examining corporations' involvement in Cyber-operations, intelligence analysis and drone piloting, and support for special forces in irregular conflicts in failing states. Finally, the third section examines how American national security agencies have altered their approach to procuring technology from corporations. In order to assure continued access to cutting-edge innovations, the United States government has adopted a venture capital model of development by partnering with the start-up business community in Silicon Valley.[15] This model allows

American national security agencies to steer nascent companies' business trajectories by influencing up-and-coming firms to apply their innovations to the field of defence.

The changing United States defence industry landscape

The United States has an extensive record of partnering with corporations in order to advance its national security interests.[16] By hiring contractors to perform non-essential duties and to supplement existing resources when the military faces production challenges and personnel shortfalls, co-operation with the private sector enables the armed forces to focus on their core responsibilities.[17] American defence contractors are generally classified by their financial size and by the types of goods and services they provide the government.[18] A significant portion of United States defence spending goes to large, publicly traded corporations traditionally associated with hardware and weapons manufacturing.[19] Some of these companies, including Lockheed Martin and General Dynamics, annually earn over $20 billion in revenue from government contracts.[20] Many corporations also supply logistics support to the armed forces.[21] Although typically smaller than hardware manufacturers, logistics specialists like Fluor and KBR—which both earned over $2 billion in federal contracts in 2019—regularly assist American military missions by providing construction, engineering, oil and gas, and maintenance services to the Pentagon.[22] Intelligence analysis and Cyber-operations are also increasingly outsourced to corporations such as SAIC and Booz Allen Hamilton, which each secured over $4.5 billion in federal contract awards in 2019.[23] In recent years, however, academic work on defence contractors has focused primarily on private military and security companies (PMSCs), which are typically smaller firms that supply protection and tactical services to government agencies and the Pentagon. More specifically, much recent literature in the field has analysed PMSC's performance in the wars in Iraq and Afghanistan from 2003–2011, with particular focus on the company formerly known as Blackwater.

While some level of defence outsourcing is to be expected—and in many instances contributes to enhancing United States national security—contractors' considerable involvement in the Iraq War, the War in Afghanistan, and numerous other post 9–11 counter-terrorism operations has prompted analysts to note the growing privatisation of the United States defence infrastructure.[24] In the conflicts in Iraq and Afghanistan, for example, personnel employed by contractors in-country regularly outnumbered members of the regular military.[25] Although contractors in Iraq and Afghanistan only occasionally became involved in firefights with insurgents, in both conflicts corporate employees regularly engaged in protection services, assisted in special operations missions, and interrogated high-value detainees.[26] Moreover, numerous companies that operated in Iraq and Afghanistan—including KBR, DynCorp, CACI, and Blackwater—were found to have overcharged the United States government and, in the case of Blackwater's employees, to have violated international law.[27] The encroachment of corporations into functions potentially deemed "inherently governmental" has resulted in extensive debate regarding the precise activities that should be considered the exclusive domain of the military and federal employees and those which can be performed by private sector employees. As defined by the Freedom from Government Competition Act (FAIR) and the Office of Management and Budget, the term "inherently governmental" refers to any duty that as a matter of law and policy must be performed by federal government employees and

cannot be contracted out because it is "intimately related to the public interest."[28] Although the exact interpretation of the term remains imprecise, there is widespread agreement amongst legal scholars that any function that could "significantly affect the life, liberty or property of private persons" should be carried out by government employees.[29] In practice, the experience of corporations providing protection services in Iraq coupled with updated legal interpretations has resulted in a sharp distinction between "warfighters"—who may use force in military operations—and contractors, whose job is to support government employees while remaining outside of activity or decisions that would involve them in the so-called "kill-chain."

Since the end of major combat operations in Iraq and Afghanistan, scholars and policy analysts have struggled to identify the changing features of the United States' defence industry. As the United States' strategic defence posture shifts away from counter-insurgency and nation-building operations and increasingly towards new forms of hi-tech warfare characteristic of the latest revolution in military affairs, government agencies responsible for national defence are demanding new types of service provision from the private sector. Despite this significant shift in the United States' strategic posture, much current research on defence outsourcing continues to examine events that took place over a decade ago in Iraq and Afghanistan. There are several understandable reasons for this pattern. When the United States was involved simultaneously in two major wars, public scrutiny of contractors was more extensive. Researchers were able to draw upon the investigative work of journalists as well as information gleaned from Congressional oversight committees in order to assess defence outsourcing practices.[30] Presently, defence contracting receives far less attention than it did when the wars in Iraq and Afghanistan were at their zeniths. Although the defence industry is changing rapidly, and United States spending on contractors continues to rise, academic analysts have largely overlooked new developments in defence markets—or have lost interest in the field altogether.[31] This is unfortunate. Because contractors remain central to American military operations and account for more than half of DoD's budget, understanding their evolving role is necessary for assessment of the United States' larger global security posture.

Although contractors' performance in Iraq and Afghanistan received heavy criticism from the media and academic community, United States military and intelligence agencies increasingly rely on corporations to support vital national security operations. This growing dependence is exemplified by rising government outlays on defence outsourcing. In 2000, the United States spent $189 billion on defence contractors. By 2017, that figure had risen 69 percent in inflation adjusted dollars to $320 billion—more than China and Russia spent on their militaries combined in that year.[32] DoD obligations to defence contractors in 2017 totalled more than all funds spent on outsourcing by all other United States government agencies combined and accounted for eight percent of all federal spending and over twenty-five percent of the country's discretionary budget.[33] The scale of DoD's recent outsourcing reinforces what many analysts and active duty military personnel already know: defence contractors have become integrated into almost all aspects of United States military operations.[34]

The $320 billion obligated to contractors by the DoD in 2017 can be broken down into three broad categories: products, services, and research and development. Products consist of the hardware—ships, unmanned aerial vehicles, missiles, etc.—the United States military uses to carry out its missions. Services involve human labour that the military employs

to assist in its operations. Finally, research and development consists of scientific investigation into new warfighting technologies. Figure 1 depicts the distribution of DoD funds across these three areas in 2017. Whilst defence outsourcing across all procurement categories warrants greater investigation, analysts are most concerned that inherently governmental responsibilities are being increasingly outsourced to corporations in the field of military and intelligence services.[35]

In 2017, DoD spent $131 billion dollars on services provided by defence contractors, representing an increase of 67 percent over outlays in 2000.[36] While demand for defence-related services is rising, the duties corporations perform have changed significantly over the past decade. When major combat operations were ongoing in Iraq and Afghanistan, contractors involved in these contingency operations were responsible for supporting United States counter-insurgency and nation-building objectives by building and managing military bases, protecting diplomatic and aid mission workers, and providing in-country logistics support.[37] However, the United States' national defence strategy has shifted since combat operations ended in Iraq and a gradual drawdown of troops began in Afghanistan. Since 2011, United States policy-makers have de-prioritised counter-insurgency and focused instead on three primary threats: (1) conflict with rival states including China, Russia, North Korea and Iran; (2) counter-terrorism and homeland security rather than counter-insurgency and nation-building; (3) Cyber-threats from both state and non-state actors.[38]

In response to this realignment of strategic priorities, defence contractors are now increasingly asked to provide a variety of more specialised services summarised collectively by military and intelligence agencies as command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). C4ISR involves the manufacture and management of hi-tech products and computer networks that assist United States armed forces in all aspects of their operations—from gathering intelligence to making battlefield decisions. A broad concept, the following list of activities would all fall under the C4ISR classification: collecting and analysing information via unmanned

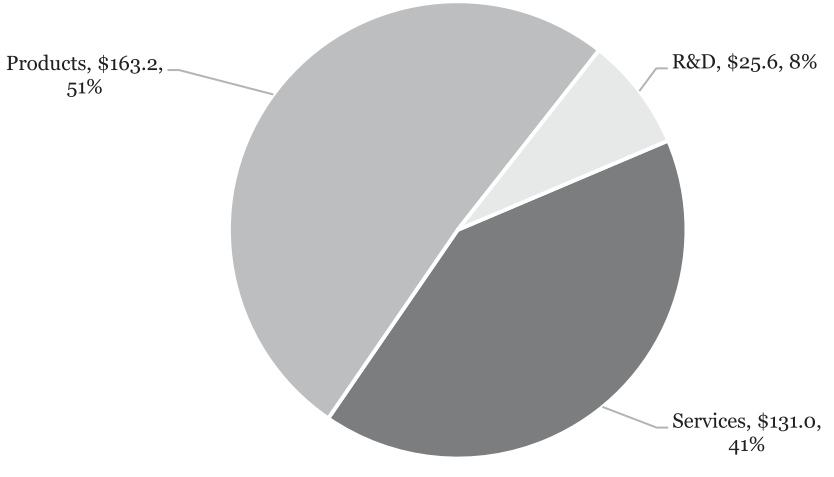

Figure 1. 2017 DoD Obligations to Defense Contractors (Billions $). Source: General Services Administration.

aerial vehicles, using satellite imagery to assess enemies' positions in the field, providing troops on the ground with tactical options for attacking enemy installations, assisting in the design and execution of both defensive and offensive Cyber-operations, designing and implementing electronic warfare weapons and operations, and developing artificial intelligence to analyse enemies' tactics. Conceivably, under the C4ISR heading, a single defence contractor could provide a spectrum of services to troops in the field and assist in all steps of the battlefield decision-making chain from reconnaissance to plan of attack.[39] American defence contractors are careful to note, however, that C4ISR activities do not involve their employees in the physical field of battle, which remains the exclusive domain of "warfighters"—a term frequently used by contractors and the military to refer to members of the armed forces.

The United States government's new strategic outlook coupled with the armed forces evolving tactical requirements have caused a major shift within the United States defence industry. Notably, the demand for protection services and support activities related to largescale troop deployments has decreased while the need for hardware and services falling under the C4ISR category has grown.[40] Furthermore, major American defence contractors are withdrawing from activities that could result in their employees engaging in physical conflict with enemy forces. The negative publicity and subsequent public backlash Blackwater experienced as a result of human rights violations committed by its employees in Iraq sent a clear message to the industry: serious repercussions may result when company employees become involved in firefights, even if contractors are attacked first and follow existing rules of engagement. George Krivo, the CEO of defence contractor DynCorp, noted this change in industry sentiment in a recent interview pointing out that his company's service offerings have changed in recent years: "DynCorp does not conduct inherently governmental functions … We do not even do private security any more … And that's a fundamental decision that we've embraced at the company in the last few years."[41]

The shift away from counter-insurgency support and protection services to C4ISR has resulted in two major industry business trends. First, large prime contractors that have traditionally supplied hardware to the DoD—including General Dynamics, Raytheon, and Northrop Grumman—are increasingly entering the defence services sector.[42] Although these major defence firms supplied much of the equipment used in the wars in Iraq and Afghanistan, they were largely absent from contingency contracts that supported in-country operations. Instead, companies including KBR, DynCorp, Fluor, Blackwater, and Triple Canopy received the lion's share of contingency contracting dollars spent in those conflicts.[43] While these are well-known names, they are small corporations relative to "big five" contractors like Raytheon and General Dynamics, which both have market valuations greater than $50 billion. Second, a wave of consolidation is taking place due to the integrated nature of C4ISR services and the market threat posed to mid-tier contractors by the incursion of larger corporations into the defence services sector.[44] The previous few years have seen several large mergers and acquisitions including Raytheon's proposed merger with United Technologies, General Dynamics' $9.7 billion deal for CSRA, SAIC's purchase of Engility for $2.5 billion, and CACI's acquisitions of LGS Innovations for $725 million and Mastodon Design for $225 million.[45]

To summarise, the services sector of the United States defence industry has undergone a rapid shift since the end of major combat operations in Iraq and Afghanistan. These

changes have largely been spurred by new demands from national security agencies, which anticipate future conflicts to be waged at least partially with autonomous weapons and in Cyber-space. In response to these new demands, defence contractors have de-prioritised supporting counter-insurgency activities and are instead focused on providing a suite of technical and data analytic services that inform and support military and intelligence operations. Collectively referred to as C4ISR, these capabilities involve contractors in a broad spectrum of activities that range from intelligence analysis to providing tactical battlefield options. While careful to draw a distinction between "warfighters" and their employees, corporations in the defence industry are now more integrated into the military operational decision-making chain than at any point in American history.

United States defence contractor involvement in ongoing conflicts

This section assesses United States contractors' roles in ongoing conflicts in three rapidly growing areas: Cyber-operations, intelligence analysis and unmanned weapons systems, and advisory forces in failing states. In each of these fields, corporations run the risk of being involved in activities that could be considered inherently governmental. That is, there exists the possibility that corporate actions could result in casualties to enemy forces or could influence decisions that result in collateral damage. By comparison, in Iraq and Afghanistan Blackwater's mandate was to protect military installations and high-ranking diplomatic and political clients. The company's employees were not expected to engage with enemy forces; instead, if attacked, their orders were to protect their clients and evacuate to safety. In practice, however, Blackwater often became involved in firefights with insurgents—blurring the line between their role as "protectors" and soldiers' role as the exclusive "warfighters." Over time, Blackwater's skirmishes with extremists led to a more aggressive corporate posture, as contractors assumed an expanded role that involved activity not permitted by their stipulated rules of engagement.[46] Similarly, in emerging fields of conflict—including Cyber—the line between offensive and defensive force is ambiguous, thus raising the potential that corporations may engage in actions that go beyond their original scope of operations and into the realm of inherently governmental activities.

Cyber-operations

Cyber-operations are central to United States national security strategy.[47] In 2017, United States Cyber Command (CYBERCOM)—the DoD's centre for managing offensive and defensive Cyber-operations – was made a unified combatant command and given the mission of training Cyber-warriors, advocating for more Cyber-security resources, and planning and conducting Cyber-operations.[48] Although Cyber-attacks resulting in human casualties have yet to occur, experts warn that destructive strikes against transportation networks, health care providers, industrial control systems, and other vulnerable targets are likely to take place in the future.[49] Moreover, United States military and intelligence agencies no longer view Cyber-operations as fundamentally defensive in nature and are rapidly developing offensive Cyber-tools to hinder enemy capabilities and even possibly to disable the communication and energy infrastructures of rival states.[50] The United States government's commitment to enhancing its Cyber-operations capabilities is

evidenced by rapidly increased spending in this area. In 2017, the United States allocated $19.8 billion for Cyber-security programmes, an increase of more than 50 percent over 2014 levels.[51]

Corporations have a major role both in implementing defensive Cyber-measures across government agencies and in developing offensive Cyber-tools for use in operations abroad. Large, publicly traded corporations including Leidos, Northrop Grumman, Booz Allen Hamilton, and General Dynamics all earned more than $1 billion in revenues from federal Cyber-security contracts during the 2018 fiscal year.[52] The labour necessary to develop both defensive and offensive Cyber-capabilities is highly specialised and in significant demand. When competing for this talent pool, contractors often can pay software engineers and network specialists significantly more than government agencies can afford. This market feature has resulted in CYBERCOM facing difficulty staffing its ranks – a workforce shortage that has been supplemented by defence contractors.[53]

Defensive Cyber-operations involve assisting United States government agencies with protection of military and intelligence computer networks as well as with securing the software that runs communications systems and hardware the armed forces use to carry out missions. Corporations have supported DoD and United States intelligence agencies with defensive Cyber-capabilities for over two decades, and thus are deeply embedded within the field. As Tim Maurer notes, a robust defensive Cyber-security market serving the private sector has existed in the United States since the late 1990s, when the internet became a major part of American business operations.[54] For this reason, partnerships between government agencies and corporations were a natural outgrowth of services many Cyber-security companies were already providing to businesses. Defensive Cyber is the largest component of the government Cyber-security market and is often carried out by major American technology companies not typically considered defence contractors like IBM and Dell.[55]

Unlike defensive Cyber-security, offensive Cyber-operations are intended to project power by applying force in and through Cyber-space and may result in casualties.[56] The United States government recently acknowledged that it had begun engaging in offensive Cyber-activities and, in recent years, defence contractors have also publicly acknowledged their role in this field.[57] Offensive Cyber is the fastest growing area of United States government Cyber-operations. In 2018, federal government spending to enhance these capabilities grew 65 percent from 2017 levels to $2.6 billion.[58] A review of many major defence contractors' corporate websites reveals that they now actively promote their ability to assist in offensive Cyber-attacks. For instance, on its website CACI advertises "offensive Cyber" as one of its services. The company notes that it "develops tools, tactics, techniques and procedures to conduct operations related to networks, end points, and connected platforms and devices."[59] Similarly, ManTech International – another publicly traded defence contractor – lists "offensive Cyber" as a service capability on its website. The corporation claims: "ManTech's offensive cyber capability is unrivalled within the intelligence community and the Department of Defense … Services include vulnerability research; reverse engineering of malware … media and hardware exploitation … and specialised mission support."[60] Other major defence contractors including Lockheed Martin, Leidos, Booz Allen Hamilton, and Northrop Grumman have also acknowledged that they now engage in offensive Cyber-operations. Some even advertise job openings for "offensive Cyber-planner" on their websites.[61]

Presently, defence contractors are primarily engaged in offensive Cyber-activities involving reconnaissance, surveillance, and intelligence gathering; however, in Cyber-space the line between distinct aspects of offensive and defensive operations remains vague.[62] Furthermore, as a new domain of warfare that is highly clandestine – with little public oversight or even knowledge of the basic types of operations United States government agencies and contractors are conducting – offensive Cyber-operations constitute an area where potential violations of domestic and international law are more likely to occur. Because offensive Cyber-operations can involve projecting force capable of causing significant damage in the physical world, corporations' involvement in this emerging domain of conflict is problematic.

Drone reconnaissance, surveillance, and intelligence analysis

Gathering accurate intelligence about an enemy's position, force size, and capabilities has always been a key element of warfare. Presently, the means by which information is collected and assessed by United States military and intelligence agencies is changing rapidly. In the past, satellite imagery and reconnaissance sorties flown by pilots were typically used to gain information about adversaries. While these methods of gathering information are effective, they are expensive and not always available when troops in the field need them immediately.[63] To solve this problem, the United States now often uses unmanned aerial vehicles (UAVs) – commonly referred to as drones – for reconnaissance, surveillance, and intelligence collection in addition to using them for missile strikes against high-value terrorist targets.[64]

Defense contractors develop and manufacture the majority of UAVs used by United States armed forces and intelligence agencies. In 2017, the total market size for military drones was estimated to be $7 billion – with Northrop Grumman and General Atomics accounting for approximately 50 percent of the supply.[65] Since at least 2010, the military has also outsourced piloting of UAVs and analysis of intelligence gathered by drones to the private sector.[66] Current estimates are that at least ten percent of the labour force analysing video surveillance sent to military and intelligence agencies by drones consists of contractors.[67] In some instances, the corporations that develop and manufacture UAVs are also responsible for supplying the labour force that pilots them. For example, in 2018 the United States Navy hired General Atomics to help fly MQ-9 Reaper drones in Afghanistan due to a shortage of available pilots within the Navy's ranks.[68] This is not an isolated incident. Both drone pilots and conventional pilots in the Navy and Air Force have become increasingly strained by multiple deployments, even as demand for reconnaissance and surveillance missions to provide intelligence about insurgents' and terrorists' activity has increased.[69] Contractors are regularly used to fill this labour shortage.

While United States law prohibits civilian personnel from piloting drones that fire weapons, contractors' assessment of intelligence provided by UAVs can place them in the so-called decision-making "kill-chain." For example, in 2010 an American Hellfire Missile airstrike killed at least fifteen civilians in a convoy in Afghanistan. An investigation of the incident determined that an analyst working for the defence contractor SAIC had mistakenly interpreted the video feed from a drone and that this flawed assessment was partially responsible for the decision to launch the attack.[70] American military lawyers have acknowledged that including contractors in the decision-making chain that results in the use of lethal

force is highly problematic for at least two reasons. First, contractors face a significant conflict of interest in these situations. As the Army Special Operations Command has noted, a contractor analysing intelligence that could lead to a strike "may be reluctant to make a definitive call, fearing liability or negative contractual action."[71] That is, contractors may place personal and corporate interests above the interests of the military. Second, some legal experts assessing contractors' role in decisions that result in missile strikes have argued that civilians who directly communicate targeting information to pilots may be in violation of international law.[72] Furthermore, the legal status of contractors involved in the drone "kill-chain" remains vague. Should a contractor violate international law as part of a decision that results in civilian casualties, it is unclear what practical legal recourse would exist to bring that individual or their corporation to justice.[73]

Security force training and special operations support in Africa

Barring a major strategic realignment, the United States government has ruled out large-scale military involvement in nation-building missions for the foreseeable future.[74] Nonetheless, counter-terrorism remains a central focus of American national security planning.[75] Although the Middle East typically dominates headlines when it comes to counter-terrorism operations, the United States now considers several countries in West Africa, the Sahel, and the Horn of Africa – including Somalia, Niger, Nigeria, Chad, Libya, Senegal, and Mali – as locations that could serve as safe havens for branches of the Islamic State, al-Qaeda, or other transnational extremist groups.[76] The United States' goal in these countries is to prevent extremists from controlling large swaths of territory that could be used to recruit, train, and plan attacks against American interests. There is also risk that extremists in Africa could cause regional destabilisation, which might eventually draw the United States into a larger war. In an effort to prevent this eventuality, the United States has deployed over 7,000 military personnel across the Sahel and the Horn of Africa with the goal of supporting the armed forces of partner host-nations. The United States has also pledged over $240 million in military aid to the region.[77] Unlike in Iraq and Afghanistan – where the United States sought to alter the political and economic structure of countries through massive military, diplomatic, and aid efforts – the United States' goal in African countries is to enhance the counter-terrorism capabilities of partner forces using a "small footprint" approach.[78]

Over 1,000 personnel employed by defence contractors are presently working alongside United States special forces personnel and troops deployed throughout Africa.[79] One of the primary functions being performed by these civilians is military training. In Somalia, for example, American corporations have worked with Marines to recruit and train soldiers for the African Union Mission to Somalia (AMISOM). Contractors have also been embedded within AMISOM units during combat operations.[80] However, unlike in Iraq and Afghanistan, where the United States' goal was to construct large national armies and police forces, in Somalia contractors are limited to developing small units with the capacity to fight the insurgent organisation al-Shabaab.[81] Training missions in Somalia are intended to be low profile. As a United States State Department official has noted: "we do not want an American footprint or boot on the ground."[82] Some of the security force training in Somalia has been conducted by Bancroft Global Development, an American-based defence contractor that has hired ex-soldiers from South Africa,

France, and several Scandinavian countries to recruit and train local forces.[83] Although in the past Bancroft has worked on the front lines with AMISOM troops involved in urban warfare against al-Shabaab, the company insists that its employees do not engage in direct combat operations, claiming that "mercenary activity is antithetical to the fundamental purposes for which Bancroft exists."[84] Presently, Bancroft's primary role in Somalia consists of recruiting and training Somali nationals to become part of an elite group of Somali Army soldiers known as the Danab, whose duty is to carry out offensive attacks against al-Shabaab.[85]

The United States military is not the only American institution involved in outsourcing security force training in Africa. In recent years, the State Department has also been handed a central role in managing counter-terrorism operations in the region as part of both the Antiterrorism Assistance Program (ATA) and the Africa Peacekeeping Program (AFRICAP).[86] To fill this role, the State Department has often turned to corporations that specialise in police training and counter-terrorism capacity-building. One such firm is Skybridge Tactical, a company formed by former green berets that focuses on developing host government security force capacity in counter-insurgency and irregular warfare.[87] According to Skybridge's website, the firm has been tasked by the State Department to "support African countries and regional organisations to enhance their capacity to prevent, manage, and resolve their own conflicts."[88] Another defence contractor tasked with providing counter-terrorism training in Africa is PAE, a Virginia-based company owned by private equity firm Platinum Equity. In 2017, PAE was the recipient of an indefinite delivery, indefinite quantity contract from the State Department to train host-nation forces in SWAT tactics and tactical responses to terrorist attacks. PAE estimates that the total value of these contract awards will be between $60–$90 million annually.[89]

In addition to training host-nation police and military in counter-terrorism tactics, defence contractors also assist American special forces units with their operations throughout the region. For example, in Niger – where over 800 American military personnel are based – contractors enter into conflict zones to support missions. In 2017, for instance, American service members undertaking a mission in Niger were ambushed by members of the Islamic State in the Greater Sahara. Four United States military service personnel were killed in the attack. As the ambush took place, Berry Aviation – a United States defence contractor that operates aircraft in support of military missions – was called upon to conduct "casualty evacuation and transport" for United States and partner forces under attack.[90] While Berry Aviation was not involved in combat activities during the ambush, it played an integral role in removing special operations troops from the battle.

To summarise, across the Sahel and Horn of Africa, defence contractors are supporting a sprawling United States effort to contain the spread of extremism. Ultimately, the extent of contractor-support will reflect the larger American military commitment to the region. However, what has become clear is that contractors are integral to the operations of United States forces in Africa and will be called upon to provide training and support services if the United States' mission expands.

Towards a venture capital model of defence procurement

The United States government's co-operation with corporations to advance American strategic defence capabilities is not a new phenomenon. However, the means by which

defence and intelligence agencies now procure technology and promote the integration of the private sector with national defence operations has changed markedly over recent decades. Specifically, rather than simply assess how ongoing technological advancements can be adapted for national security purposes – or rely on traditional prime defence contractors to develop new technologies – the United States government now actively funds start-up companies to develop tools that can be applied for defence and intelligence operations. To achieve this goal, the government has adopted a business model used by the venture capital community with the goal of gaining access to emerging technologies at their earliest stages of development. Perhaps no better exemplar of this practice exists than In-Q-Tel (IQT), a strategic investment firm created by the Central Intelligence Agency (CIA) and funded by United States national security agencies and given the mission of accelerating the delivery of cutting-edge technologies from the private sector to the defence community.[91]

IQT was formed out of a recognition within the American defence community that the United States government was no longer a central actor in technological R&D.[92] During the Cold War, American government agencies were among the world's leading scientific organisations. NASA's space programme and DARPA's development of the technology that would become the internet were just two of many government programmes demonstrating that state-led research could result in breakthrough innovation.[93] However, in the 1980s the personal computing revolution and emerging business opportunities in related technology ventures resulted in a brain drain away from government as the private sector became the United States' primary locus of scientific progress.[94] This transition meant that national security agencies could be prevented from adapting innovations for defence activities if corporations did not co-operate with the government. Agencies, including the CIA, whose reputations had been damaged during the Cold War, often found it difficult to form partnerships with technology companies that stylised themselves as iconoclastic and employed generally progressive workforces.[95]

In response to this problem, in 1999 the CIA formed IQT to access and influence technologies being developed by start-up businesses. In essence, IQT acts as a venture capital firm, providing nascent companies with capital to fund operations and R&D. However, IQT differs from traditional venture capital in two ways. First, because the organisation is funded by the government and earnings from investments are not distributed to partners, it is technically a non-profit entity.[96] Second, because IQT's clients are government agencies, its interest is not necessarily to maximise the commercial viability of the companies it invests in, but rather to ensure that technologies developed by firms in its portfolio can be applied to defence operations. Therefore, early investment from IQT may shift corporations' R&D trajectories towards creating products that can be used by military and intelligence agencies rather than by public consumers or corporations.

Since its inception, IQT has invested in over 400 companies in hi-tech fields including Cyber-security, artificial intelligence, biotechnology, data-analytics, and space operations.[97] To gain access to these emerging firms, IQT has established offices in global technology hubs including Silicon Valley, Boston, London, and Sydney. Some of IQT's notable investments include: FireEye, a Cyber-security firm that specialises in preventing malware attacks; Cloudera, a data-analytics company developing machine learning tools; and RedSeal, a company focused on securing cloud computing applications. However, IQT's most high-profile – and controversial – investment is in big data firm Palantir

Technologies, which specialises in predictive data-analysis. Today, Palantir's software tools – originally intended to help defence agencies identify and prevent terrorist threats – are increasingly being used by domestic law enforcement to surveil American citizens.[98]

Palantir was formed in 2003 by PayPal founder and libertarian activist Peter Thiel. Thiel's original vision for Palantir was to apply fraud recognition technology developed by PayPal to national security challenges, especially those related to counter-terrorism.[99] IQT was one of Palantir's earliest backers, initially investing in the company in 2005 after several traditional venture capital firms had declined to support the firm.[100] IQT also served as a conduit between Palantir and its first major client: the CIA. In Palantir's early years, the CIA was the company's primary customer, helping keep Palantir afloat while the company developed intelligence applications for its data-mining algorithms. By 2009, CIA special forces units in Iraq and Afghanistan had begun to use Palantir's software to track insurgent movements and predict where roadside bombs might be placed.[101] The successful application of Palantir's software by special forces was noted by the military, and in 2011 Marines in Helmand and Nimroz provinces in Afghanistan began using Palantir's tools to collect biometric information from explosive devices in order to chart insurgents' bomb-making networks.[102] After 2011, versions of Palantir's analytic software quickly made their way through the national security community as the company won contracts from the FBI, Defense Intelligence Agency, and Department of Homeland Security.

Just a decade after its formation, Palantir began competing with prime defence contractors for major Army contracts. By 2015, Palantir had developed a version of its software that could be used by troops in the field to analyse intelligence, visualise enemy positions, and provide tactical response options. Palantir's software represented direct competition to the Army's existing Distributed Common Ground System (DCGS), which was largely developed and maintained by defence contractor Raytheon. After a lengthy bidding process, which involved Palantir suing the Army for what it considered unfair procurement practices, in 2019 Palantir won an $800 million contract to revamp the DCGS and became the first Silicon Valley company to win a "defence programme of record," a designation reserved for the largest and most important defence contracts.[103] Palantir has since won an $80 million award from the United States Navy, firmly establishing itself as a major DoD contractor.[104]

Palantir's analytic software, originally used by the CIA to identify terrorist and insurgent threats, is now widely employed not only by the military but also by businesses and law enforcement. For instance, JPMorgan has employed Palantir's tools to identify potential fraud and intellectual property theft. Meanwhile, police forces including the Los Angeles Police Department and the New York Police Department, use Palantir's software to track gang activity and to identify individuals that the software predicts are likely to break the law.[105] The software's growing use in the defence and business sectors has resulted in a rising corporate valuation, with analysts predicting that Palantir's eventual IPO will value the company at over $25 billion.[106]

To summarise, Palantir's business trajectory represents a new model of co-operation between United States national security agencies and technology start-ups. Notably, while traditional prime contractors like Raytheon and Northrop Grumman still receive the lion's share of government defence spending, the increasing importance of Cyber-

security, data-analytics, and machine learning in military operations signifies that tools developed by tech companies outside the traditional Beltway defence industry are increasingly relevant to United States national security. Early investment from the CIA's strategic investment firm IQT helped legitimize Palantir, bringing in a wave of interest from more traditional venture capital firms. Meanwhile, cooperation with the CIA in Afghanistan enabled Palantir to refine its software to the specific needs of the defence community. Following this incubation period, Palantir's software has spread rapidly within American defence agencies and the company stands to become one of the largest IT defence contractors after its eventual IPO. More concerning, Palantir's recognition and data analytics tools are now being used within the United States by Immigration and Customs Enforcement (ICE) and metropolitan police departments to track the undocumented as well as to surveil civilians who may not have committed any crimes.[107] While Palantir's growth has been swift, it certainly is not an outlier. IQT has invested in over 400 start-ups, and its success in helping American defence agencies access new technologies signifies that the United States' new model of venture capital defence development is firmly established.[108]

Conclusion

The United States government spent over $200 billion on defence contractors during major combat operations in the wars in Iraq and Afghanistan.[109] The most comprehensive review of the quality of defence outsourcing during these wars – carried out by the Congressional Commission on Wartime Contracting in Iraq and Afghanistan – reached a stark conclusion: "The Commission's conservative estimate of waste and fraud [during both wars] ranges from $31 billion to $60 billion."[110] Furthermore, contractors supplying protection services in these conflicts were severely criticised for taking part in inherently governmental, quasi-combat operations. Blackwater, the firm that received the most public scrutiny for its actions, changed its name twice in an effort to rebrand itself, and several of its employees were found guilty of either murder or manslaughter.[111] Other contractors including KBR, DynCorp, and CACI were involved in documented incidents of wrongdoing and fraud.[112] Based on the American experience with contractors in Iraq and Afghanistan, United States reliance on defence outsourcing after 2011 could be expected to diminish. However, while American contractors have generally moved away from performing quasi-combat responsibilities in warzones, they have become no less essential in short-term and long-term United States operational planning.

Since the completion of major combat operations in Iraq in 2011, the United States' broad strategic objectives have altered considerably. Nation-building in the Middle East via the application of counter-insurgency techniques is no longer a priority – or fiscally practical. Instead, United States defence posture has shifted to focus on Cyber-threats, counter-terrorism rather than counter-insurgency, and possible conflict with states including China and Russia. This change in American strategy has resulted in demands for new types of services from defence contractors, whose role in future military operations remains central to DoD planning. Most notably, contractors are supplying much of the specialised, highly-skilled labour needed to develop and use hi-tech tools that will form the backbone of future military operations. As technology becomes more central to warfare, contractors' role in American defence operations is likely grow. The

United States government has a long history relying on corporations to develop weapons systems and communications infrastructure; however, as combat evolves, the Pentagon will require more software engineers, drone pilots, and highly trained intelligence analysts to support its "warfighters."

Defense contractors are also deeply embedded within the United States' economy. In recent decades, publicly traded corporations in the defence industry have grown to become a major part of the manufacturing sector as well as mainstays in the stock portfolios of many Americans. With respect to manufacturing, roughly ten percent of total United States factory output goes into the production of weapons sold primarily to the DoD.[113] This involves numerous companies – not all directly related to the defence industry – that provide raw materials, shipping, and other important business services and inputs to defence contractors. Any major alterations in defence procurement will thus affect not only contractors, but a host of ancillary actors that serve the broader defence industry. In the domain of finance, the defence sector has become a key element in the stock portfolios of many institutional and individual investors. The stocks of major contractors such Boeing, Lockheed Martin, and Raytheon are regularly analysed on financial news programmes on CNBC and Bloomberg Television as well as in major publications like the Wall Street Journal and Forbes. The sector is often portrayed as stable by analysts, who argue that predicting contractors' revenues is fairly straightforward because defence budgets typically do not fluctuate drastically from year to year and demand for goods and services remains consistent.[114] Furthermore, significant barriers to entry in much of the industry make defence contractors relatively immune to disruption from upstart companies, thus making the sector an attractive option for investors. To summarise, defence contractors are embedded within the United States economy and their collective financial performance affects a broad range of individuals and corporations. For this reason, a major change in defence procurement policy or a reallocation of defence funds to alternative areas of government spending has the potential to reverberate throughout the American economy.

Finally, the United States is not unique in recognising the growing importance of private sector innovations to enhancing military capacity. China and Russia have also harnessed the power of corporations in efforts to advance their strategic interests, albeit using distinct methods. The future of warfare, therefore, is likely to be characterised by a clash of corporations as great powers work in tandem with defence contractors and multinational companies in an effort to become the globe's dominant technological and military actors.

Notes

1. United States Department of Defense, *2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (2018). https://www.hsdl.org/?view&did=807329.
2. Adam Taylor, 'The Pentagon says China and Russia are Bigger Problems for U.S. Than Terrorists', *The Washington Post*, January 20, 2018. This viewpoint has become even more widespread since the United States military and its allies retook territory controlled by the Islamic State (IS) in Iraq and Syria as part of Operation Inherent Resolve.
3. Elbridge Colby, 'How to Win America's Next War', *Foreign Policy*, May 5, 2019; Michael McFaul, 'A Grand Strategy for Confronting Putin', *Foreign Affairs*, July/August 2018; Robert S. Ross, 'US Grand Strategy, the Rise of China, and US National Security Strategy

for East Asia', *Strategic Studies Quarterly* 7, no. 2 (2013): 20–40; United States National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*, 2018, https://www.usip.org/publications/2018/11/providing-common-defence.

4. United States Department of Defense, *2018 National Defense Strategy of the United States of America* (2018).
5. Warren Chin, 'Technology, War, and the State: Past, Present, and Future', *International Affairs* 95, no. 4 (2019): 765–83.
6. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014); P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin, 2009); Laura Dickinson, 'Drones, Automated Weapons, and Private Military Contractors: Challenges to Domestic and International Legal Regimes Governing Armed Conflict', in *New Technologies for Human Rights Law and Practice*, eds. Molly K. Land and Jay D. Aronson (Cambridge: Cambridge University Press, 2018), 93–124; Jon R. Lindsay, 'Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations', *The Journal of Strategic Studies* 36, no. 3 (2013): 422–53, James Johnson, 'Artificial Intelligence and Future Warfare: Implications for International Security', *Defense & Security Analysis* 35, no. 2 (2019): 147–69.
7. In 2011, the bipartisan Congressional Commission on Wartime Contracting in Iraq and Afghanistan (CWC) found that 'poor planning, management, and oversight of contracts has led to 'massive waste' and 'damaged' vital United States national interests. United States Government Commission on Wartime Contracting in Iraq and Afghanistan, *Transforming Wartime Contracting: Controlling Costs, Reducing Risks* (Washington, D.C.: United States Congress, 2011).
8. Moshe Schwartz, John F. Sargent Jr., and Christopher T. Mann, *Defense Acquisitions: How and Where DoD Spends Its Contracting Dollars* (Washington, DC: Congressional Research Service, 2018), 1–3; United States Department of Defense, 'Department of Defense (DoD) Releases Fiscal Year 2017 President's Budget Proposal', February 9, 2016.
9. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2017); Dana Priest and William M. Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little Brown and Company, 2011); Michael S. Schmidt, 'Air Force, Running Low on Drone Pilots, Turns to Contractors in Terror Fight', *The New York Times*, September 5, 2016.
10. DynCorp, for instance, no longer supplies private services to the Pentagon or State Department.
11. Constellis, the company that formed from the merger of Blackwater and Triple Canopy, recently defaulted on its credit obligations due to a lack of business from the DoD. See Stephen Gandel, 'Owner of Former Blackwater Defense Contractor in Danger of Bankruptcy', *CBS News*, January 6, 2020.
12. On the legal definition of inherently governmental functions see John R. Luckey, Valerie Baily Grasso, and Kate M. Manuel, *Inherently Governmental Functions and Department of Defense Operations: Background, Issues, and Options for Congress* (Washington, DC: Congressional Research Service, 2009).
13. Heidi M. Peters, Moshe Schwartz, and Lawrence Kapp, *Department of Defense Contractor and Troop Levels in Iraq and Afghanistan: 2007–2017* (Washington, DC: Congressional Research Service, 2017), 1–2.
14. Charles W. Mahoney, 'Acquire or Expire: Publicly Traded Defense Contractors, Financial Markets, and Consolidation in the United States Defense Industry', *Defence and Peace Economics* (2019).
15. Both the CIA and DoD have created organizations intended to serve as investment vehicles and, in essence, 'bridges' between the defence community and Silicon Valley. The CIA's nonprofit, venture capital firm is called In-Q-Tel (https://www.iqt.org) and the DoD's is called the Defense Innovation Unit (https://www.diu.mil).

16. Harvey M. Sapolsky, Eugene Gholz, and Caitlin Talmadge, *U.S. Defense Politics: The Origins of Security Policy* (New York, NY: Routledge, 2017); Eugene Gholz, 'The Curtis-Wright Corporation and Cold War-Era Defense Procurement: A Challenge to Military Industrial Complex Theory', *Journal of Cold War Studies* 2, no. 1 (2000): 35–75; Raphael S. Cohen, 'Putting a Human and Historical Face on Intelligence Contracting', *Orbis* 54, no. 2 (2010): 232–51.
17. Raymond Franck and Francois Melese, 'Defense Acquisition: New Insights from Transaction Cost Economics', *Defense & Security Analysis* 24, no. 2 (2008): 107–28.
18. For a classification system based on service provision type see P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2003).
19. Bloomberg Government, *BGOV200: Federal Industry Leaders 2019* (New York, NY: Bloomberg, 2019).
20. Ibid.
21. When the military operates overseas, logistics support is often provided by foreign contractors. For more on logistics support of United States military operations see Adam Moore, *Empire's Labor: The Global Army That Supports U.S. Wars* (Ithaca, NY: Cornell University Press, 2020).
22. Bloomberg Government, *BGOV200: Federal Industry Leaders 2019*.
23. Priest and Arkin, *Top Secret America*.
24. Allison Stanger, *One Nation Under Contract: The Outsourcing of American Power and the Future of American Foreign Policy* (New Haven, CT: Yale University Press, 2009); Laura A. Dickinson, *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs* (New Haven, CT: Yale University Press, 2011).
25. Heidi M. Peters, Moshe Schwartz, and Lawrence Kapp, *Department of Defense Contractor and Troop Levels in Iraq and Afghanistan: 2007–2017* (Washington, DC: Congressional Research Service, 2017).
26. On the definition of mercenaries and the distinction between mercenaries and employees of defence contractors see Sarah Percy, *Mercenaries: The History of a Norm in International Relations* (New York: Oxford University Press, 2007); Hin-Yan Liu and Christopher Kinsey, 'Challenging the Strength of the Antimercenary Norm', *Journal of Global Security Studies* 3, no. 1 (2018): 93–110.
27. United States Government Commission on Wartime Contracting in Iraq and Afghanistan, *Transforming Wartime Contracting*, 38–98; United Nations Human Rights Office of the High Commissioner, 'Blackwater Sentencing—UN Experts on Mercenaries Call for International Regulation of Private Security', April 15, 2015, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15840&.
28. Luckey, Grasso, and Manuel, *Inherently Governmental Functions and Department of Defense Operations*, p. 1. For more on increased defence outsourcing see Trevor Taylor, 'Private security companies in Iraq and beyond,' *International Affairs* 87, no. 2 (2011): 445–565; Deborah Avant, *The Market for Force: The Consequences of Privatizing Security* (Cambridge, MA: Cambridge University Press, 2005); Sean McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order* (New York, NY: Oxford University Press, 2014); Charles W. Mahoney, 'Buyer Beware: How Market Structure Affects Contracting and Company Performance in the Private Military Industry', *Security Studies* 26, no. 1 (2017): 30–59.
29. Kate M. Manuel, *Definitions of Inherently Governmental Function in Federal Procurement Law and Guidance* (Washington, DC: Congressional Research Service, 2014).
30. Well-known journalistic works on military and intelligence contracting include *Jeremy Scahill, Blackwater: The Rise of the World's Most Powerful Mercenary Army* (New York: Nation Books, 2007); Priest and Arkin, *Top Secret America*.
31. This is not necessarily true of think-tanks, which continue to investigate weapons manufacturing and the United States defence industrial base. For example, see the Center for Strategic

& International Studies' Defense-Industrial Initiatives Group: https://www.csis.org/programs/international-security-program/defence-industrial-initiatives-group.
32. Schwartz et al., *Defense Acquisitions*, 1–2.
33. United States Congressional Budget Office, 'Discretionary Spending in 2018: An Infographic', https://www.cbo.gov/publication/55344.
34. Brigadier General Jeffrey A. Doll, 'Operational Contract Support Needs a Joint Force Focus', *Army Sustainment*, July 5, 2017, https://www.army.mil/article/189268/operational_contract_support_needs_a_joint_force_focus.
35. Stanger, *One Nation Under Contract*; Dickinson, *Outsourcing War and Peace*; Ulrich Petersohn and Molly Dunigan, *The Markets for Force: Privatization of Security Across World Regions* (Philadelphia, PA: University of Pennsylvania Press, 2015).
36. Schwartz et al., *Defense Acquisitions*, 1–2.
37. United States Government Commission on Wartime Contracting in Iraq and Afghanistan, *Transforming Wartime Contracting*, 23–5.
38. United States National Defense Strategy Commission, *Providing for The Common Defense,* 6–11.
39. For example, Northrop Grumman claims to specialize in all aspects of C4ISR. See Northrop Grumman's corporate website: http://www.northropgrumman.com/capabilities/c4isr/Pages/default.aspx.
40. Mark Hoover, 'Do You Know How to Navigate Today's Defense Market?' *Washington Technology*, November 6, 2014; *MarketWatch*, 'C4ISR Market is Anticipated to be Worth US $132.26 Billion by 2026', November 21, 2018.
41. Joe Gould, 'DynCorp CEO George Krivo Talks Sale Rumors, Its Rebound, and Blackwater', *DefenseNews*, October 10, 2018. https://www.defencenews.com/digital-show-dailies/ausa/2018/10/10/interview-dyncorp-ceo-george-krivo-on-sale-rumors-its-rebound-and-blackwater/.
42. William Welsh, 'Raytheon Doubles Down on Cybersecurity', *Washington Technology*, June 16, 2015.
43. United States Government Commission on Wartime Contracting in Iraq and Afghanistan, *Transforming Wartime Contracting*, 25.
44. Greg Nossaman, 'M&A Opportunities Abound in Changed Market', *Washington Technology*, February 23, 2017.
45. Ross Wilkers, 'SAIC to Acquire Engility', *Washington Technology*, September 10, 2018; Aaron Mehta, 'General Dynamics Completes CSRA Acquisition', *DefenseNews*, April 3, 2018.
46. Renée De Nevers, 'Private Security Companies and the Laws of War', *Security Dialogue* 40, no. 2 (2009): 169–90.
47. United States Department of Defense, *2018 National Defense Strategy of the United States of America*.
48. United States Department of Defense, 'Cybercom to Elevate to Combatant Command', May 3, 2018.
49. Amy Zegart and Michael Morrell, 'Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail', *Foreign Affairs*, May/June 2019, 85–96; Tarah Wheeler, 'In Cyberwar, There are No Rules', *Foreign Policy*, September 12, 2018.
50. Michael Sulmeyer, 'Military set for Cyber Attacks on Foreign Infrastructure', Belfer Center for International Security, April 11, 2018; Michael Sulmeyer, 'How the U.S. Can Play Cyber Offense', Belfer Center for International Security, March 22, 2018.
51. Govini, *Federal Cybersecurity: FY18 Standard Market Taxonomy of Unclassified Spending*, 1. https://www.govini.com/federal-cybersecurity-fy18-standard-market-taxonomy-of-unclassified-spending/.
52. Govini, *Federal Cybersecurity*, 2–21.
53. Irv Lachow and Taylor Grossman, 'Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations', in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, eds. Herbert Lin and Amy Zegart (Washington D.C., Brookings Institution Press, 2018), 387.
54. Maurer, *Cyber Mercenaries,* 71.

55. Govini, *Federal Cybersecurity*, 4.
56. United States Joint Chiefs of Staff, *Cyberspace Operations: Joint Publication 3-12*, June 8, 2018, II-5.
57. Warren P. Strobel, 'Bolton Says U.S. is Expanding Offensive Cyber Operations', *The Wall Street Journal*, June 11, 2019.
58. Govini, *Federal Cybersecurity*, 1.
59. CACI corporate website: http://www.caci.com/cyber_security/capabilities.shtml.
60. ManTech corporate website: https://www.mantech.com/capabilities/cyber.
61. Booz Allen Hamilton corporate website: https://careers.boozallen.com/en-US/job/offensive-cyber-operations-planner/J3P3KL6N8MG0HSZ7JVC.
62. Eric Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyber Space', *Security Studies* 24, no. 2 (2015): 316–48.
63. Mark Bowden, 'How the Predator Drone Changed the Character of War', *Smithsonian Magazine*, November, 2013.
64. For research on the United States' drone operations against insurgent and terrorist organizations see Patrick B. Johnston and Anoop K. Sarbahi, 'The Impact of US Drone Strikes on Terrorism in Pakistan', *International Studies Quarterly* 60, no. 2 (2016): 203–19. For more information and data on United States Drone Strikes see New America Foundation, *America's Counterterrorism Wars*, https://www.newamerica.org/in-depth/americas-counterterrorism-wars/.
65. Michael Peck, 'Four Companies Dominate the Military Drone Market', *C4ISR.net*, April 6, 2016.
66. Michael S. Schmidt, 'Air Force, Running Low on Drone Pilots, Turns to Contractors in Terror Fight', *The New York Times*, September 5, 2016; David S. Cloud, 'Civilian Contractors Playing Key Roles in U.S. Drone Operations', *Los Angeles Times*, December 29, 2011.
67. Cloud, 'Civilian Contractors Playing Key Roles in U.S. Drone Operations'.
68. Joseph Trevithick, 'U.S. Navy Wants to Hire Contractors to Fly Their Own MQ-9 Reaper Drones in Afghanistan', *The Drive*, January 10, 2018.
69. Stephen Losey, 'More Time at Home? Air Force Seeks to Ease Relentless Deployments for In-Demand Airmen', *Air Force Times*, January 18, 2018.
70. Cloud, 'Civilian Contractors Laying Key Roles in U.S. Drone Operations'.
71. Ibid.
72. There is significant legal debate over this issue. See Charles Kels, 'Contractors in the "Kill-Chain"? At the Nexus of LOAC and Procurement Law', *Lawfare*, January 24, 2016.
73. The legal means to address violations of international law by employees of defence contractors has been an important area of academic concern. For instance, see Kristine A. Huskey, 'Accountability for Private Military and Security Contractors in the International Legal Regime', *Criminal Justice Ethics* 31, no. 3 (2012): 193–212.
74. Andrew Tilghman, 'After 15 Years of War, America's Military Has About Had It with Nation Building', *Military Times*, September 22, 2016.
75. United States Department of Defense, *2018 National Defense Strategy of the United States of America*.
76. Jessica Donati, 'As Diplomacy Shifts, U.S. Expands Military-Style Counterterrorism Training', *The Wall Street Journal*, May 6, 2019; Manni Crone, 'Islamic State's Incursion into North Africa and Sahel: A Threat to Al-Qaeda?', *Connections: The Quarterly Journal* 16, no. 1 (2017): 63–76.
77. Katie Bo Williams, 'From Small Wars to Great Power, Trump's Africa Reset Could Change Military's Role', *Defense One*, December 12, 2018; Council on Foreign Relations, 'The Risks of Reducing U.S. Special Operations in Africa', September 13, 2018; Eric Schmitt, 'Where terrorism is Rising in Africa and the U.S. is Leaving', *The New York Times*, March 1, 2019.
78. Alexis Okeowo, 'The Enduring American Military Mission in Africa', *The New Yorker*, May 2, 2017.
79. Dan Lamothe, 'Pentagon Grapples with a Thorny Question After Niger Ambush: What Next in Africa?', *Washington Post*, March 19, 2018.

80. Mark Mazzetti, Jeffrey Gettleman, and Eric Schmitt, 'In Somalia, U.S. Escalates a Shadow War', *The New York Times*, October 16, 2016.
81. Ibid.
82. Jeffrey Gettleman, Mark Mazzetti, and Eric Schmitt, 'U.S. Relies on Contractors in Somalia Conflict', *The New York Times*, August 10, 2011.
83. Kyle Rempfer, 'US Troops, Nonprofit Trainers and a "Lightening Brigade" Battle for Somalia', *Military Times*, May 21, 2019.
84. Gettleman, Mazzetti, and Schmitt, 'U.S. Relies on Contractors in Somalia Conflict'.
85. Rempfer, 'US Troops, Nonprofit Trainers and a "Lightening Brigade" Battle for Somalia'.
86. Donati, 'As Diplomacy Shifts, U.S. Expands Military-Style Counterterrorism Training'.
87. Skybridge Tactical Corporate website: https://skybridgetactical.com/skybridge-focus-areas/training-support.
88. Skybridge Tactical corporate website: https://skybridgetactical.com/skybridge-contracts/africa-peacekeeping-program.
89. 'PAE awarded Global Anti-Terrorism Assistance IDIQ Contract and Three Regional Task Orders', PAE Corporate Website, September 27, 2017. https://www.pae.com/news/pae-awarded-global-anti-terrorism-assistance-idiq-contract-and-three-regional-task-orders.
90. Joseph Trevithick, 'U.S. Military Reveals Contractors Flew to the Rescue in Niger, but Little Else', *The Drive*, October 17, 2017.
91. Rick E. Yannuzzi, 'In-Q-Tel: A New Partnership Between the CIA and the Private Sector', *Defense Intelligence Journal* 9, no. 1 (2000).
92. John T. Reinert, 'In-Q-Tel: The CIA as Venture Capitalist', *Northwestern Journal of International Law & Business* 33, no. 3 (2013): 677–709.
93. Yannuzzi, 'In-Q-Tel'.
94. Ibid.
95. United States military and intelligence agencies still struggle to secure partnerships with firms such as Google. See Zegart and Morrell, 'Spies, Lies, and Algorithms', 95.
96. Although it is a non-profit, any returns IQT earns from its investments are available for use in future investments. See Reinert, 'In-Q-Tel', 698.
97. IQT corporate website: https://www.iqt.org/iqt-through-the-years/.
98. Peter Waldman, Lizette Chapman, and Jordan Robertson, 'Palantir Knows Everything About You', *Bloomberg Businessweek*, April 19, 2018.
99. Andy Greenberg, 'How a Deviant Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut', *Forbes*, September 2, 2013.
100. Ibid.
101. Ken Dilanian, 'US Special Operations Forces are Clamoring to Use Software from Silicon Valley Company Palantir', *Business Insider*, March 26, 2015.
102. Palantir, 'Fielding an Advanced Analytic Capability in a Warzone', https://www.palantir.com/_ptwp_live_ect0/wp-content/uploads/2012/06/ImpactStudy_USMC.pdf.
103. Shane Harris, 'Palantir Wins Competition to Build Army Intelligence System', *The Washington Post*, March 26, 2019.
104. Aaron Gregg, 'Palantir Seals Its First Major U.S. Navy Deal as Raytheon is Passed Over', *The Washington Post*, March 5, 2020.
105. Waldman, Chapman, and Robertson, 'Palantir Knows Everything About You'.
106. *CNBC*, 'Palantir to Seek at Least $26 Billion Valuation in Fundraising Push', September 20, 2019.
107. April Glaser, 'Palantir Said It Had Nothing to Do with ICE Deportations. New Documents Seem to Tell a Different Story', *Slate*, May 2, 2019.
108. IQT's successful model of accessing technology from the private sector has been partially imitated by the Pentagon, which in 2016 announced the formation of Defense Innovation Unit Experimental (DIUx), a DoD organization tasked with helping the military gain access to cutting-edge technological innovation in the private sector. For more on DIUx see Aaron Metha, 'Former Symantec Boss Takes Over at Defense Innovation Unit', *DefenseNews*, September 24, 2018.

109. United States Government Commission on Wartime Contracting in Iraq and Afghanistan, *Transforming Wartime Contracting*, 25.
110. Ibid., 5.
111. Thomas Jackman and Spencer S. Hsu and, 'Blackwater Security Guard Convicted in 2007 Iraqi Civilian Massacre at Third U.S. Trial', *Washington Post*, December 19, 2018.
112. United States Government Commission on Wartime Contracting in Iraq and Afghanistan, *Transforming Wartime Contracting*.
113. Louis Uchitelle, 'The U.S. Still Leans on the Military-Industrial Complex', *The New York Times*, September 22, 2017.
114. For example, see Phillip van Doorn, 'Aerospace and Defense Sector May Keep Flying High for Years to Come', *MarketWatch*, September 19, 2018.

Acknowledgements

The author would like to thank Ulrich Petersohn, Christopher Spearin, Benjamin Tkach and other participants in the University of Liverpool's 2019 workshop on private military and security companies and civil war.

Disclosure statement

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

Notes on contributor

Charles W. Mahoney is Associate Professor in the Department of Political Science at California State University, Long Beach. He holds PhD and MA in Political Science from UCLA and BA with highest honors in History from Williams College. His research focuses primarily on non-state actors in international security settings, with special emphasis on defence contractors and extremist organizations. Dr Mahoney's work has appeared in numerous scholarly journals. He is presently working on a book examining changes within the United States defence industry since the 9/11 terrorist attacks.