STRATEGIC STUDIES QUARTERLY - PERSPECTIVE

Corporate Hackers: Outsourcing US Cyber Capabilities

Charles W. Mahoney

Abstract

Cyberspace is a key war-fighting domain that affects all aspects of United States national security. Although defense contractors are essential to United States cyber operations, little research has examined the specific cyber services military and intelligence agencies outsource to corporations. This article evaluates government contracting practices in three strategically important United States cyber markets: cybersecurity, offensive cyber operations, and data analytics. Each market possesses distinct structural economic features that affect cyber outsourcing. After almost two decades of contracting, the cybersecurity market functions efficiently because it is competitive and information about the capabilities of corporate suppliers is widely available. Conversely, the small number of suppliers in the offensive cyber market coupled with the limited commercial utility of offensive cyber tools suggests that the sector may develop into an oligopoly in which the United States government is highly dependent on contractors. Finally, data analytics is a relatively new field comprised of numerous corporate suppliers that possess limited experience working with the Department of Defense and the intelligence community. Lack of information about companies' relative capabilities in the data analytics market means that government agencies are likely to make suboptimal contracting decisions when choosing among prospective suppliers.

*****

Cyberspace is a key war-fighting domain that affects all aspects of United States national security.[1] Although defense contractors are essential to United States cyber operations, little research has examined the specific cyber services military and intelligence agencies outsource to corporations.[2] Furthermore, the nature of contracting between government agencies and corporate cyber service providers remains understudied.[3] What types of cyber operations do defense contractors carry out for United States military and intelligence agencies? Is United States cyber outsourcing efficient? That is, do government agencies accurately identify the most qualified cyber service providers, capably monitor their behavior, and foster competitive markets that encourage innovation while keeping costs affordable?

This article argues that structural economic differences in three distinct cyber markets—cybersecurity, offensive cyber operations, and data analytics—have important implications for the quality of outsourcing carried out by United States defense and intelligence agencies. In the cybersecurity market, which has existed for over 20 years, contracting is relatively efficient. The market is characterized by numerous suppliers, and government agencies possess detailed information about corporations' capabilities and past performances. By contrast, the emerging market for offensive cyber operations has a small number of suppliers, and the tools companies develop for offensive cyber missions have limited utility outside national security settings. These two factors are likely to lead to an inefficient market in which government agencies are highly dependent on contractors. Finally, the market for "big data" analytics—which involve collection, analysis, and visualization of information using algorithms—is relatively new. Thus, the Department of Defense (DOD) and intelligence community have little experience assessing the capabilities of competing firms. This feature of the analytics market means that government agencies are more likely to make suboptimal choices when assessing the relative capabilities of companies in the field. However, the competitive nature of the analytics market coupled with the wide applicability of analytics products outside defense-specific settings suggests that assessment and oversight of firms will become more efficient as information about companies increases through repeated contracting.

This article first describes three key United States defense markets for cyber operations and identifies the major companies active in each market. Next, it presents concepts from transaction cost economics and applies this body of theory to government outsourcing in the cybersecurity, offensive cyber, and data analytics markets. The article then examines two important cases of United States government cyber contracting: The Department of Homeland Security's $1 billion Development, Operations, and Maintenance (DOMino) contract and the United States Army's $876 million Distributed Common Ground System A-2 (DCGS-A2) contract. The conclusion summarizes major findings and presents policy recommendations for future military and intelligence cyber outsourcing.

Defense Contracting and United States Cyber Operations

American military and intelligence agencies have an extensive history of procuring goods and services from corporations.[4] By outsourcing nonessential duties and hardware production to contractors, the national security community can more efficiently focus on its core strategic planning and war-fighting responsibilities. Additionally, companies are an important source of technological innovation for the armed forces.[5] Although partnership with the private sector is a key pillar of American national defense, in recent decades the government has increasingly outsourced vital national security functions historically carried out by Soldiers and civilian government employees.[6] As a recent Congressional Research Service report notes, "without contractor support, the United States would not be able to arm and field an effective fighting force."[7]

Cyber operations are an emerging field in which the DOD and the intelligence community are highly integrated with the private sector and where contractors perform mission critical functions. In 2017, the United States government authorized $19.8 billion in unclassified spending for all cyber related activities performed by defense contractors, an increase of 120 percent over 2012 levels.[8] Scholars have advanced several typologies to classify varying types of cyber operations. While academic debate in this area is likely to persist, there is emerging consensus that distinct differences exist among cybersecurity—which includes defensive cyber operations,[9] offensive cyber operations, and data analytics.[10] What follows is an analysis of outsourcing in these three strategically important cyber markets.

Cybersecurity

The Joint Chiefs of Staff define *cybersecurity* as activities that protect United States government data, networks, and cyberspace-enabled hardware by defeating malicious cyber activity carried out by adversaries.[11] Various technical responsibilities fall within the broad category of cybersecurity, including providing network defense, software application security, protection of command and tactical communications, and hardware and infrastructure protection against electronic attacks. The central objectives of cybersecurity operations are to protect United States government computers and electronic communication systems and to ensure that military and intelligence agencies possess data availability, integrity, and confidentiality.[12]

Among the three main categories of cyber operations, cybersecurity comprises the largest share of federal government spending, accounting for 75 percent of funds spent on all outsourced cyber activities related to national defense between 2012 and 2017.[13] The corporations receiving the bulk of defense-related funding for cybersecurity operations during this period include Northrop Grumman, Lockheed Martin, Perspecta, IBM, Dell, General Dynamics, Leidos, Booz Allen Hamilton, Raytheon, CACI, and SAIC.[14] These companies provide "full spectrum" cybersecurity capabilities. That is, they offer government agencies a suite of services ranging from network risk analysis and cyber threat anticipation through cyber incident response and digital forensics. For example, Booz Allen Hamilton uses "cyber fusion centers" to support the DOD and intelligence community with services including vulnerability assessment, threat prevention, red team testing, and cyberattack detection and response.[15] Similarly, Leidos offers full-spectrum cyber services using a "security operations center" approach that supports government agencies by detecting, managing, and responding to cyber threats. The largest corporations providing the federal government with cybersecurity services employ thousands of specialists whose skills are in high demand. General Dynamics alone employs over 3,000 cyber professionals who work with government agencies in an effort to improve the nation's defensive cyber capabilities.[16] By comparison, the United States Cyber Command (CYBERCOM)—the DOD's organizational hub for coordinating the military's cyber operations—presently has approximately 1,000 full-time military and civilian staff members.[17]

A notable feature of the cybersecurity market is the recent entrance of prime defense contractors, traditionally associated with hardware production, into the sector. In part, prime contractors' shift into cybersecurity has occurred out of necessity. As hardware becomes increasingly integrated with applications that run in cyberspace, corporations must ensure that the satellite systems, planes, drones, and tanks they produce are "cyber resilient" against enemy attack. However, many major contractors—including Raytheon, Northrop Grumman, and Lockheed Martin—have also begun providing government agencies with cybersecurity services not directly associated with the hardware they design and build. Raytheon, for example, supplies cybersecurity services to the Department of Homeland Security and other government agencies as part of the $1 billion DOMino contract.[18] Northrop Grumman, another major manufacturer of military hardware, recently won an Air Force contract to provide CYBERCOM with rapid access to a "full spectrum of cyber capabilities."[19]

Another significant trend in cybersecurity operations is the emergence of major commercial technology companies as suppliers to the national security community. In the past, technology firms often were reluctant to work with the DOD and CIA for fear of damaging their brands. In recent years, however, Amazon, Microsoft, and Oracle have become direct competitors to traditional federal information technology (IT) contractors in certain cybersecurity service areas, particularly network and cloud security.[20] In 2013, for example, Amazon won a $600 million contract to modernize the CIA's computer networks.[21] As part of this transition, Amazon was responsible for securing sensitive information stored and operated in its cloud platform. Amazon has publicly acknowledged that the defense industry represents a major focus of its future strategic business plans: "The defense, intelligence, and national security communities deserve access to the best technologies in the world[,] . . . and we [Amazon] are committed to supporting their critical missions."[22] Another high-profile example of commercial technology firms' rise in the cybersecurity market is the Pentagon's Joint Enterprise Defense Infrastructure (JEDI) project, a $10 billion contract that attracted proposals from Amazon, Microsoft, Google, IBM, and Oracle. The JEDI project tasks one company with managing the DOD's transition from traditional to cloud-based computer systems. A central part of this transition involves securing classified Pentagon information stored in cloud networks.[23] Microsoft was awarded the JEDI contract in 2019; however, Amazon is actively contesting the award.[24]

Offensive Cyber Operations

Cybersecurity operations protect United States government computer networks. By contrast, offensive cyber operations seek to penetrate enemy cyberspace and, at times, to impair adversaries' hardware and critical physical infrastructure.[25] The Joint Chiefs of Staff note that all cyber operations conducted outside of "blue cyberspace"—areas in cyberspace protected by the government and its mission partners—are classified as offensive cyber operations.[26] Therefore, causing kinetic damage is not a necessary criteria for a cyber operation to be considered offensive in nature. In fact, much offensive cyber activity carried out by the DOD and the intelligence community consists of efforts to gather intelligence, with no intent to cause immediate physical or functional damage to adversaries' computer systems or infrastructure. These types of nondestructive offensive cyber operations are referred to as "cyber exploitation" and constitute the primary activity of defense contractors operating in the offensive cyber market.

In 2017, federal spending on offensive cyber activities outsourced to contractors totaled $2.6 billion, an increase of 65 percent over 2016 outlays.[27] Contractors' offensive cyber activities include environment preparation and cyber tools development, which both involve penetration of adversaries' computer networks. Environment preparation consists of efforts to penetrate enemy cyberspace in order to evaluate the capabilities, intentions, and potential threats posed by adversaries.[28] Environment preparation can be considered surveillance and reconnaissance in cyberspace and is key to the DOD's "defend forward" approach to cyber threats, which stresses halting malicious cyber activity at its source.[29] Cyber tools development entails creating code and applications that can be used to access and potentially damage enemy networks, hardware, and infrastructure. Defense contractors that support cyber tools development are often referred to as "offensive cyber operations planners" and assist the DOD and intelligence agencies in the design phase of offensive cyber missions. Although some contractors are increasingly willing to acknowledge that they take part in offensive cyber operations, most maintain that they neither build cyber weapons nor direct offensive cyber operations. According to company representatives, both of these activities remain the exclusive responsibility of the military and the intelligence community.[30]

Defense contractors active in the offensive cyber market include Northrop Grumman, Booz Allen Hamilton, ManTech International, CACI, General Dynamics, Leidos, Lockheed Martin, BAE Systems, and SAIC. The private sector market for offensive cyber is relatively new, and corporations doing business in the field have only recently publicly acknowledged their role in these operations.[31] Some companies now overtly advertise their offensive cyber capabilities. ManTech International, for instance, claims that its "offensive cyber experience is unrivaled within the Intelligence Community and Department of Defense" and that the company provides services including "vulnerability research" and "media and hardware exploitation."[32] CACI touts an "expert offensive cyber operations team" that provides support against "adversarial platforms."[33] In contrast to ManTech and CACI, SAIC is less overt about its offensive cyber work; however, the company frequently advertises job openings for "offensive cyber planners" on its website, and SAIC executives have acknowledged that the offensive cyber market is an important growth area for the company.[34]

From the vague language that corporations publicly use to describe their offensive cyber services, it is evident that this area of operations is highly classified and also represents a potential legal and public relations challenge for contractors. Because offensive cyber operations involve missions that infiltrate adversaries' cyberspace, they represent behavior that could be considered "inherently governmental"[35]—that is, duties that by United States law or policy must be performed by federal government employees.[36] In the Iraq War and the war in Afghanistan, several defense contractors—most notably Blackwater—were alleged to have engaged in activities that constituted inherently governmental functions.[37] Since that time, government agencies have sought to delineate clearly those activities that must remain the responsibility of government personnel and those that contractors can perform. In kinetic domains, this has resulted in a clear distinction between Soldiers—whose responsibilities may entail physical violence or kill-chain decisions—and contractors, who are not permitted to directly take part in activity that may "significantly affect the life, liberty or property of private persons."[38] In the emerging domain of offensive cyber operations, the activities that constitute inherently governmental functions remain less clearly defined. This may pose a challenge in the future if contractors assist government agencies with cyber missions that result in casualties or significant damage to physical infrastructure.

Data Analytics and Machine Learning

The third major area of government spending on cyber capabilities is in the field of data analytics, which is closely related to machine learning and artificial intelligence. This emerging service area involves data mining, predictive algorithms, and visualization tools that can inform both kinetic and cyberspace missions.[39] Thus, while traditional cyber operations form part of the data analytics field, the potential applications of data analytics tools are extremely diverse. In the realm of cybersecurity, analytics applications use algorithms to gather information about cyber threats in order to identify and neutralize malicious code. Analytic cyber tools may also be offensive in nature, such as Russia's use of automated malware in recent cyberattacks against Ukraine.[40] Within the national security community, agencies are increasingly turning to machine-led data analysis to assist in mission critical decision-making.[41]

In 2017, the federal government spent $1.4 billion on services provided by contractors to enhance analytics and machine learning capabilities related to cyber operations.[42] These services include incident response and forensics, continuous diagnostics and mitigation, and data visualization.[43] Leading companies in this field include Palantir, KBR, Raytheon, Perspecta, and Booz Allen Hamilton.[44] The market for machine learning–supported cyber tools is dynamic and includes numerous start-up companies that supply a variety of different services. More so than other cyber markets, advances in machine learning technologies are taking place at corporations not considered pure-play defense contractors. This reality has altered traditional DOD methods of procurement and has caused established defense contractors to anticipate challenges from upstart firms. To gain a foothold in the data analytics market, many existing corporations in the defense industry have pursued strategic acquisitions.[45] For instance, in 2018 Perspecta—formerly the public-sector services division of DXC

Technology—acquired Vencore and Keypoint, two smaller firms specializing in machine learning and cybersecurity. With these acquisitions, Perspecta leveraged its existing relationships with the DOD and the intelligence community to rapidly become one of the leading cyber data analytics suppliers in the defense industry. Similarly, KBR—a company primarily known for its oil and gas logistics capabilities—acquired data analytics firm Stinger Ghaffarian Technologies (SGT) for $355 million in 2018. KBR now brands itself as a leader in big data, artificial intelligence, and machine learning and is focusing much of its future business on cyber operations in addition to its core energy services enterprise.

In contrast to Perspecta and KBR, data analytics firm Palantir has its roots in the Silicon Valley start-up community. Established in 2003 by a group of investors that included PayPal co-founder Peter Thiel, in its early years Palantir was supported by investments from CIA-backed venture capital organization In-Q-Tel.[46] In the wars in Iraq and Afghanistan, Palantir's software was used by both the CIA and Marine Corps to support counterterrorism missions.[47] Since the late 2000s, Palantir's analytic tools—which involve data mining, predictive algorithms, and data visualization—have been adopted by numerous defense and intelligence agencies as well as by private sector businesses.[48] Palantir's Gotham platform is used by the intelligence community to analyze "data sources, unstructured cable traffic, structured identity data, email, telephone records, spreadsheets, [and] network traffic" to inform intelligence analysis.[49] Similarly, Palantir's Phoenix and Hercules systems are used for cybersecurity by government agencies and the private sector and employ data mining and machine learning technologies to autonomously identify and mitigate cyber threats.[50] The company's rapid rise within the United States defense community has resulted in a corporate valuation of over $45 billion, and it is now a publicly traded corporation.[51]

Although data analytics and machine learning presently represent a small segment of the United States cyber services market, technological advances in the field have the potential to affect the global balance of power.[52] This prospect is supported by the substantial investment countries are making in artificial intelligence technologies. China, for instance, is a world leader in facial recognition capabilities and has identified artificial intelligence as an "existential priority."[53] Similarly, Russian president Vladimir Putin famously asserted that whatever state becomes dominant in artificial intelligence "will be the ruler of the world."[54] While machine learning has utility in traditional defensive and offensive cyber operations, its potential applicability to numerous other facets of military planning and operations—both in cyberspace and in physical domains—is broad. For this reason, the market for data analytics and machine learning services is perhaps the most lucrative and strategically important cyber sector going forward.

Transaction Cost Economics and Defense Contracting

This inquiry applies two related bodies of theory, transaction cost economics and principal-agent theory, to explain features of United States cyber outsourcing. Both areas of knowledge examine relationships in which a principal, often a corporation or government agency, enters into a contractual relationship with a second organization—the agent—tasked with providing a good or service to the principal in exchange for a fee. According to these theories, both corporations and government bureaucracies regularly procure goods and services from outside suppliers because they confront the "make or buy" decision.[55] That is, organizations must determine what goods and services they can efficiently produce internally and what inputs and operations are more efficiently supplied to them by the market via contracting.[56] In the context of defense outsourcing, this question can be reframed by asking, What services—excluding inherently governmental functions—are most effectively performed by Soldiers and government employees, and which are more efficiently supplied to the DOD and the intelligence community by the private sector?[57]

A central assumption in both principal-agent theory and transaction cost economics is that participants in any contractual agreement are limited by imperfect information. This bounded rationality signifies that all complex, long-term contracts are inherently incomplete and contain what economist Oliver Williamson refers to as "gaps, errors, and omissions" that may result in varying interpretations of a contract's meaning.[58] In business relationships governed by contracts, several potential inefficiencies—referred to as transaction costs—may result from imperfect contracts. For example, in the contract bidding phase, principals may make suboptimal decisions when choosing among potential suppliers. This "adverse selection" results from information asymmetries that exist between principals and agents with respect to the capabilities of companies competing for a contract award. In the execution phase of a contract, principals often face challenges assessing agents' performance.[59] Because principals usually cannot monitor the totality of agents' activities—and may even lack the expertise to effectively evaluate agents' output—they inevitably allot a degree of "agency slack" to contracted firms.[60] Finally, even if principals find that agents have shirked their obligations, it can be difficult for them to enforce agreements because of the imprecise nature of contracts' language and the costs associated with finding an alternate supplier or seeking financial recompense in the courts.

An additional inefficiency that may arise in outsourcing results from variation in asset specificity. Asset specificity refers to transaction costs that occur due to the nature of the products and services being exchanged between buyers and sellers and the potential for these products and services to be redeployed for other purposes.[61] If asset specificity is low, goods and services produced as part of a contractual agreement can be redeployed easily for alternative purposes by different users without significant reduction of value. However, if goods and services arising from a contractual agreement are highly specialized—and have little utility outside an existing contractual arrangement—asset specificity is high and may result in increased levels of dependency by one or both parties due to sunk costs associated with the contract.[62]

Asset specificity can take numerous forms; among those most commonly identified in previous literature are human asset specificity and physical asset specificity.[63] Human asset specificity refers to skills, knowledge, experience, and intellectual property that are unique to a bilateral contractual relationship.[64] In agreements characterized by high human asset specificity, knowledge-related products that emerge from a contract are limited in use outside a unique buyer-supplier relationship. Physical asset specificity refers to products and equipment used to fulfill the terms of a contractual agreement. Physical goods designed for a specific transaction that cannot be redeployed for other economic purposes are characterized by high asset specificity.[65]

To reduce the transaction costs associated with outsourcing, principals often adopt a number of strategies. Chief among these is repeating contractual agreements with the same supplier. In many instances, transaction costs associated with outsourcing can be reduced if screening and oversight regimes between buyers and sellers are standardized over time.[66] Frequent transactions improve monitoring ability and reduce information asymmetries, allowing principals to more accurately assess the performance of agents. However, recurring contracting may also lead to alternate types of inefficiencies. Foremost among these hazards is the possibility that buyers will no longer seek competitive bids for a specific good or service due to the perceived costs of screening alternate suppliers. Therefore, in some cases, failure to engage in competitive bidding in an effort to reduce transaction costs may inadvertently result in adverse selection.

Previous literature examining defense outsourcing through the lens of transaction cost economics has identified several important characteristics of American defense markets that make contracting in the industry unique. First, many markets for defense-related goods and services are monopsonies.[67] That is, the government is the dominant buyer in the field and can use its leverage to influence contracting processes and aspects of corporations' market conduct.[68] Second, adverse selection occurs frequently in defense procurement because government agencies lack sufficient technical knowledge to discern accurately the capabilities of rival firms competing for contract awards.[69] Adverse selection may occur even in mature weapons acquisition and hardware markets due to the rapidly changing nature of some technologies. To reduce information asymmetries, government agencies often seek repeated contracting with the same corporations. This trend toward frequency, however, can lead to bilateral monopolies, which may result in agency dependence on a single contractor.[70] Third, asset specificity presents particular challenges to the defense industry. Many goods and services produced from agreements between government agencies and defense contractors have high asset specificity, meaning they have limited practical value outside their existing contractual arrangements.[71] As previous research has noted, much military training has limited applicability in commercial markets, and certain military hardware such as missiles, tanks, and submarines has almost no use outside national defense settings.[72]

To summarize, contractual agreements between government agencies and companies comprise the primary framework used to manage defense outsourcing. Transaction cost economics and principle-agent theory—two bodies of research previously used to assess the contracting practices of government bureaucracies—provide a useful foundation to explain the behavior of corporations and features of markets within the American defense industry. While previous research has leveraged these theories to examine defense procurement broadly, analysts have not used transaction cost economics to assess the markets for cyber operations, which possess characteristics that make them distinct from other sectors of the defense industry.

Theorizing Contracting Efficiency in United States Cyber Markets

As outlined in the previous section, contracting efficiency varies based on the number of buyers and sellers in a market, a market's maturity, and the types of goods and services being exchanged. Competitive markets in which buyers and sellers have longstanding relationships and where goods exchanged can be easily repurposed are likely to be efficient. By contrast, nascent markets with few suppliers and high levels of asset specificity are more likely to be characterized by high transaction costs. This section identifies the structural economic features of the cybersecurity, offensive cyber, and data analytics markets and uses this information to develop theory about how these markets function. Table 1 summarizes these arguments.

Table 1. Contracting efficiency in US national security cyber markets

		Adverse Selection	
		Low	High
Asset Specificity	High		Offensive Cyber Operations
	Low	Cybersecurity	Data Analytics/Machine Learning

Because the federal market for cybersecurity has existed for over 20 years—allowing for frequent interactions between corporations and government agencies responsible for American national security—outsourcing in this market is likely to be characterized by low levels of adverse selection.[73] Furthermore, repeated agreements between federal agencies and major defense contractors operating in the cybersecurity market reduce information asymmetries and allow for regularized monitoring and assessment regimes to exist. Additionally, asset specificity in the cybersecurity market is likely to be low because technologies developed for defensive cyber operations can be redeployed for commercial use in the private sector and for use in government agencies outside the national security community. For all these reasons, transaction costs in the cybersecurity market are likely to be low. This does not signify that adverse selection will never occur in the cybersecurity market; however, the structural features of the field indicate that it will operate more efficiently than other national security cyber markets.

In contrast to the cybersecurity market, the offensive cyber market is likely to be characterized by significant transaction costs due to high levels of adverse selection and high asset specificity. Contractors have participated in offensive cyber operations for only a few years. This limits information about companies' comparative capabilities and increases the possibility that information asymmetries exist between government agencies and suppliers. Additionally, asset specificity in the offensive cyber market is likely to be high because offensive missions often involve development of unique code used to enter the cyberspace of disparate adversaries. For this reason, the tools created as part of offensive cyber contracts have limited applicability outside their specific mission environments. Additionally, because the field is highly classified and involves covert operations in which corporations help government employees penetrate the cyberspace of adversaries—including rival states—many companies will refrain from entering the offensive cyber market. Furthermore, participation in the market is limited by legal barriers such as the Computer Fraud and Abuse Act (CFAA), which restricts offensive cyber operations to United States government entities and their mission partners.[74] Therefore, as the offensive cyber market develops, it will exhibit only moderate levels of competition and is likely to become an oligopoly on the supply side.

Finally, the market for data analytics is likely to be characterized by moderate transaction costs. More so than other federal cyber markets, data analytics has seen the rapid emergence of start-up firms that specialize in niche services. Because the application of machine learning technologies to cyber operations is a new field, adverse selection in the market is likely to be high. Furthermore, because machine learning has a broad range of applications in both cyber and kinetic domains, outsourcing will likely take place with many different companies across numerous national security agencies. In this type of market, agencies are apt to make suboptimal contracting decisions because they lack information about suppliers that comes through years of repeated contracting. However, unlike in the offensive cyber market, asset specificity in the analytics market is low because the tools and technologies developed by companies have broad use in commercial sectors. This market feature means that neither bilateral monopolies nor government dependence on a small number of contractors is likely to develop. Therefore, as contracting in the field becomes more routinized over time, adverse selection in the data analytics market should decrease, and the market will function more efficiently.

Evaluating the Theory by Examining Bid Protests

This inquiry empirically assesses one type of transaction cost present in government cyber markets: adverse selection. Measuring adverse selection can be challenging because the concept possesses an implied counterfactual. That is, an assertion that adverse selection has occurred in a contract award infers that another company could have executed the contract's terms in superior fashion for the same cost.[75] Of course, this type of claim is not verifiable unless an agency hires multiple contractors to perform an identical task for the same fee—an event that rarely occurs outside the early stages of R&D projects or weapons prototyping.[76] In United States defense procurement, however, a formal review process exists whereby companies may protest contracting decisions made by government agencies. If a company believes that an agency has made an error in its award decision, it may file a bid protest with the United States Government

Accountability Office (GAO), which then reviews the contract solicitation process in an "objective, independent, and impartial" manner.[77]

A bid protest automatically halts implementation of a contract until the dispute is reviewed and closed by the GAO.[78] If the GAO finds that a government agency acted improperly or violated federal procurement law as part of the award process, it may sustain a protest and subsequently issue appropriate corrective action, which can include termination of an improperly awarded contract. The GAO's oversight function serves as an internal check on government contracting inefficiencies, especially with respect to adverse selection. Cases in which the GAO sustains protests—such as for lack of fair competition or for incorrect assessment of companies' technical capabilities—strongly indicate that adverse selection has occurred in the procurement process.

If the GAO denies a protest, companies may still seek relief in the courts. The United States Court of Federal Claims (COFC) hears cases in which corporations believe that procurement law or policy has been violated by a government agency. While relatively few companies file complaints with the COFC, it stands as a second level of review and oversight for government contracting award decisions. If the COFC sides with a company opposing a contract awarded by a government agency, then it is likely that adverse selection occurred in that award. Decisions rendered by the COFC are considered final and are almost never appealed to the United States Court of Appeals or United States Supreme Court.[79]

Bid protest decisions are useful in assessing the prevalence of adverse selection in defense outsourcing. By examining decisions in which the GAO or COFC sustain challenges from protesting companies, government agencies can identify weaknesses in their procurement practices. By contrast, denied protests serve as evidence that agencies are carrying out thorough contract award practices. Transaction cost economics suggests that adverse selection is more prevalent in the data analytics and offensive cyber markets and less widespread in the cybersecurity market. The subsequent section evaluates these expectations by reviewing two significant cases of cyber outsourcing that underwent bid protests.

Case Studies in United States Cyber Outsourcing

The GAO and COFC together review thousands of bid protests annually; however, all defense contracts are not equal in terms of their strategic importance. A majority of bid protests are initiated by businesses seeking to reverse decisions on relatively small-dollar awards.[80] While adverse selection may occur across all types and sizes of contracts, suboptimal award decisions have the greatest potential to influence American national security on large contracts that outsource key defense responsibilities to corporations. For that reason, this inquiry reviews two major cyber contracts tasking companies with core national security duties. Each case serves as a test to determine if adverse selection occurred during the contract bidding phase. The two contracts examined are the Department of Homeland Security's (DHS) $1.15 billion DOMino contract and the Army's $875 million DCGS-A2 contract.

With respect to market type, DOMino is a cybersecurity contract while DCGS-A2 is a data analytics contract. Therefore, the article assesses outsourcing in two distinct cyber markets. While the DHS's original decision was upheld by the GAO in the DOMino award, the COFC agreed with a complaint filed against the Army on the DCGS-A2 contract. Therefore, evidence exists that a suboptimal contracting decision was made on the DCGS-A2 analytics contract, while the GAO's decision in denying a protest on the DOMino award indicates that the correct decision was made on that cybersecurity contract. These findings support arguments previously advanced in the inquiry that predict efficient contracting in the cybersecurity market and less efficient contracting in the field of data analytics.

Ideally, the market for offensive cyber services would also have been examined in this study; however, to date there are no publicly available bid protest decisions for offensive cyber contracts.[81] Activities within the offensive cyber field remain highly classified, and information about the private sector's involvement in offensive cyber operations is therefore limited. Although this inquiry cannot empirically evaluate offensive cyber outsourcing, it is the first study to develop a theoretical framework for assessing economic aspects of the offensive cyber market. In the future, as additional information about offensive cyber outsourcing becomes available, the theory advanced in this article can undergo empirical assessment.

Finally, while the two case studies in this section provide supporting evidence for the inquiry's arguments, they do not serve as a comprehensive test of the article's theoretical claims. Rather, the case studies are exploratory in nature and serve to advance theory development by identifying contracting processes in cyber markets that may lead to inefficient outsourcing.[82] Further investigation of additional cases across the cybersecurity, offensive cyber, and data analytics markets is necessary to evaluate the study's broader assertions. Despite this limitation, the arguments presented in the article serve as an important initial effort to explain features of the markets for defense-related cyber operations performed by corporations.

Development, Operations, and Maintenance Contract

The DOMino contract is a five-year, $1.15 billion cybersecurity award that tasks a corporation with defending over 100 federal computer networks from cyberattacks.[83] The DHS first issued the DOMino request for proposal (RFP) in 2014. The project tasked a contractor to assist the DHS with the design, deployment, operation, and maintenance of the National Cybersecurity Protection System (NCPS), an "integrated system of intrusion detection, analytics, information sharing, intrusion prevention, and core infrastructure capabilities that are used to defend the Federal Executive Branch civilian government's [information technology] infrastructure from cyber threats."[84] The NCPS is essentially an expansive firewall that defends all civilian federal agencies with the .gov domain from malicious cyber activity.[85]

In the DOMino RFP, the DHS highlighted several criteria used to evaluate companies' proposals. Four criteria dealt with technical aspects of DOMino's implementation. These included characteristics of the NCPS system design, ability to integrate the NCPS's capabilities across agencies, operations procedures, and staffing capacity. Additionally, the DHS specified that past contractor performance would be used to assess competing bids. The DHS received proposals from five companies.[86] While the identity of all bidders was not made public because the DOMino review process was managed by the Office of Selective Acquisitions—which supports classified procurements for the DHS—it has been reported that General Dynamics, Leidos, and Lockheed Martin were vying for the award in addition to two publicly confirmed bidders, Raytheon and Northrop Grumman.[87]

In 2015, the DHS awarded the DOMino contract to Raytheon, but Northrop Grumman quickly challenged the award. Northrop's initial challenge resulted in the DHS reevaluating its decision; however, after two reassessments the DHS reaffirmed its award to Raytheon. Northrop subsequently issued another bid protest with the GAO, arguing that awarding DOMino to Raytheon was improper for a number of reasons. Some of Northrop's complaints addressed alleged technicalities and claims of impropriety by Raytheon; however, a significant portion of the protest's content concerned issues related to past performance. Specifically, the DOMino RFP prioritized previous experience in cybersecurity operations "conducting relevant and recent work of the same and or similar nature to the requirements described in the solicitation."[88] Northrop contended that Raytheon had not demonstrated the ability to execute a cyber contract of DOMino's "scope and complexity."[89] Thus, a central component of Northrop's complaint maintained that Raytheon was a suboptimal prospective supplier because there was insufficient past information establishing that the company could execute a large cyber contract. In effect, Northrop asserted that an information asymmetry existed between the DHS and Raytheon, indicating that it was not possible for the DHS to accurately assess Raytheon's cybersecurity capabilities on a large-scale contract. According to Northrop, Raytheon's lack of previous experience increased the probability that selecting Raytheon to implement DOMino would be an instance of adverse selection.

The GAO's response to Northrop's bid protest evaluated the claim that Raytheon's previous cybersecurity contracting provided insufficient information about the company's ability to execute the DOMino contract. In its evaluation, the GAO noted that Raytheon had relevant experience on three large government cybersecurity projects within the previous five years, collectively totaling $629 million.[90] The GAO also concurred with the DHS's determination that Raytheon's recent cybersecurity work demonstrated "the offeror's ability to successfully perform work under a high dollar value contract."[91] The GAO additionally remarked that Raytheon had performed cybersecurity operations for the FBI and the National Geospatial Intelligence Agency and agreed with the DHS's assessment that this work possessed "the same complexity and scope as the anticipated cybersecurity and operations and management work under the RFP."[92] In brief, in assessing Northrop's claim that Raytheon had insufficient recent experience working on large cybersecurity contracts, the GAO found "no basis to conclude" that the DHS's initial determinations about Raytheon's capabilities were flawed.[93] For this reason, the GAO denied Northrop Grumman's protest, and the DOMino contract was officially awarded to Raytheon.[94]

To summarize, Northrop Grumman challenged the DHS's award of the $1.15 billion DOMino cybersecurity contract to its competitor Raytheon on the grounds that Raytheon had not demonstrated the ability to execute a large cybersecurity project. However, because the federal cybersecurity market has been in existence for decades and numerous companies in the field have worked on prior contracts, government agencies have substantial information about suppliers' capabilities. Therefore, when reviewing proposals, the DHS was able to assess information about contractors' past cybersecurity performance and capabilities. The GAO's review of Northrop's bid protest found that Raytheon had previously executed large cybersecurity contracts of similar scope and scale to DOMino and, based on Raytheon's previous work, agreed with the DHS that the company had the capacity to execute DOMino. While there is no definitive way to know that Raytheon was a superior supplier to Northrop Grumman, the GAO's review of the DHS's award procedure, coupled with the fact that both the DHS and GAO had substantial information about Raytheon's and Northrop Grumman's cybersecurity capabilities, reduces the likelihood that adverse selection occurred as part of the DOMino contract award process.

Distributed Common Ground System 2 Contract

The Army issued the DCGS-A2 RFP in December 2015. The contract is an extension of the DCGS-A Increment 1 (DCGS-A1) contract, which called for the development of a mobile intelligence, surveillance, and reconnaissance (ISR) analytics platform of software and hardware that would improve Soldiers' "seeing and knowing" on the battlefield—augmenting troops' situational awareness and thus enhancing tactical options and combat capabilities.[95] The DCGS system is intended to combine "all intelligence software/hardware capabilities within the Army into one program."[96] Thus, it is an analytics platform that can both analyze and visualize data, providing troops in the field and Army command personnel with vital ISR information in real time via a shared network. The Army views successful implementation of the DCGS as essential to its missions and deploys the system worldwide in all theaters of operation.[97] The system is therefore a key cyber component of United States national security operations.

DCGS-A1 comprised initial efforts to develop and implement the DCGS system. Principal companies involved in the program included Lockheed Martin and Raytheon, which both worked for over a decade on the project.[98] Although DCGS-A1 resulted in the development and deployment of an operational platform for troops on active duty, its introduction into the battlefield was met with negative assessments. For instance, after the platform was made available to units in Afghanistan, Soldiers from the 130th Engineering Brigade reported that the software was "unstable, slow . . . and a major hindrance to operations."[99] The Army Test and Evaluation Command reviewed initial iterations of the DCGS and found them to have "limitations"; it determined that the system had "poor reliability" and was ultimately "not survivable" due to its excessive complexity and "network vulnerabilities."[100] In 2014, after numerous software updates attempting to fix the DCGS platform, an internal Army review found that the system could not consistently print documents, locate files, maintain a functioning server, or perform search functions.[101] As a result of DCGS-A1's shortcomings, the DCGS-A2 solicitation called for "development of a new data architecture" that would include cutting-edge "analytical tools, cloud computing, and 'big data' analytic capabilities."[102]

Before the Army could review offerors' proposals for DCGS-A2, Palo Alto–based technology firm Palantir Technologies Inc. submitted a pre-award bid protest to the GAO. Palantir argued that the terms of the DCGS-A2 RFP were illegal because they expressly prohibited use of a commercially available product as part of the DCGS's core system.[103] This provision would prevent Palantir from competing for the DCGS-A2 award.[104] Rather than developing an entirely new data analytics platform, Palantir argued that its existing product—Palantir Gotham—was already in use by several defense and intelligence agencies and could be adjusted to perform the core analytic functions outlined in the DCGS-A2 RFP. From Palantir's perspective, adoption of an existing software platform with a proven record of success represented a superior option for the Army versus creating an entirely new DCGS system.[105]

Palantir made two claims about adverse selection in its protest. First, the company argued that a data analytics system it had already developed was superior to the existing DCGS and would be superior to competitors' efforts to develop a new system. Second, Palantir claimed that selecting a commercially available "off the shelf" system would save the Army both time and money because less labor would be required to modify an existing platform than to develop a new DCGS system from scratch.

Palantir's pre-award bid protest was denied by the GAO; however, the company subsequently sued the Army in the COFC, asking for an injunction halting solicitation on the DCGS-A2 contract.[106] In the suit, Palantir elaborated on arguments it made to the GAO, stressing that its existing software could meet most of the contract's provisions. Specifically, Palantir included testimony from engineers who had reviewed the DCGS-A2 RFP and had knowledge of Palantir Gotham's data analytic capabilities. In assessing Palantir's ability to meet the DCGS-A2 contract's key terms, one expert concluded, "All of these capabilities are available through the commercial marketplace—at a minimum, they are available from Palantir, which is able to provide each of these functions through the Palantir Gotham platform."[107] As it had previously argued to the GAO, Palantir also contended that developing a new data architecture platform from scratch "will result in failure" and will "lock the Army into an irrelevant and unusable 'flagship' intelligence architecture for the next decade."[108]

In November 2016, the COFC ruled in Palantir's favor and issued an injunction ordering the Army to cease procurement efforts for the DCGS-A2 contract until its solicitation terms complied with United States law and allowed commercially available products to be considered for the award.[109] In its decision, the COFC found that even the Army's own technical experts could not conclusively refute Palantir's ability to perform most duties outlined in the DCGS-A2 RFP.[110] Furthermore, the COFC noted that "it would be wise for the Army to seriously consider reviewing the commercially available products of Palantir, or any other potential offeror, before concluding that no commercially available product can meet the Army's requirements."[111] Therefore, while the COFC did not assert that Palantir Gotham represented a superior product, it ordered the Army to open the DCGS-A2 award to competition so that a more thorough evaluation of all potential offerors' capabilities could take place. The COFC's order thus implied that without increased competition the likelihood of adverse selection was high.

In 2018, after revising the DCGS-A2 RFP to allow companies with commercially available software to compete for the award, the Army chose Palantir and Raytheon—among eight original offerors—to demonstrate their prototypes to Soldiers in a simulated battlefield exercise.[112] After receiving feedback from Soldiers and reviewing proposals from both companies, in 2019 the Army awarded the DCGS-A2 contract to Palantir.[113] In 2020, Palantir was subsequently chosen to continue work on the DCGS system through an $823 million extension known as Capability Drop 2.[114] The company was also recently awarded its first major contract with the Navy, again defeating Raytheon to implement a data analytics project.[115]

In summary, the application of data analytics to military and intelligence operations is an emerging cyber service area. Because it is a relatively new market, government agencies have limited information about corporations' capabilities. Palantir's potential exclusion from consideration for the DCGS-A2 contract meant that the Army would have failed to evaluate a proposal from a qualified supplier that had existing business with the CIA and United States Special Operations Command. This increased the likelihood that adverse selection could occur. If Palantir had not ultimately protested the RFP's terms in court, the DCGS-A2 contract could have been awarded to an inferior supplier, and a clear instance of adverse selection would have taken place. This might have seriously hampered the Army's efforts to develop a state-of-the-art data analytics and visualization platform.

Conclusion

Cyber operations represent the latest strategic domain in which United States military and intelligence agencies have outsourced key national security responsibilities. This inquiry argues that outsourcing across all cyber markets is not identical. This reality should inform policy makers' management of this growing service area. Cybersecurity is the most developed and competitive cyber market and thus poses the lowest risk for inefficient outsourcing. Owing to decades of repeated contracting, information about the capabilities of corporations active in the cybersecurity market is readily available. Consequently, government agencies outsourcing cybersecurity capabilities are less likely to make suboptimal choices when selecting suppliers and are better able to monitor contractors' performances after agreements are executed. Conversely, the offensive cyber operations market is a new service area with only a small number of companies active in the field. Additionally, the tools that firms develop as part of offensive cyber operations have limited applications outside national security settings. For these reasons, the offensive cyber market risks developing into an oligopoly: a market structure that increases government dependence on a small number of firms. Finally, like the offensive cyber market, the application of data analytics and machine learning to defense and intelligence operations is a new field. For this reason, information about companies' relative capabilities is difficult for government agencies to assess accurately, signifying that rates of adverse selection are likely high. However, there are numerous suppliers in the data analytics market, and services provided by companies in the sector have utility outside national defense settings. Thus, contracting efficiency in the analytics market should improve over time.

Going forward, American leaders must make important policy choices about the trajectory of cyber outsourcing. Two key policy guidelines emerge from this study's arguments. First, outsourcing offensive cyber operations poses both economic and legal risks. The structure of the offensive cyber market and the nature of the tools produced in the field predispose it to inefficiency. Legally, contractors risk taking part in inherently governmental functions if their work on offensive cyber missions directly results in casualties. This means defense agencies should retain—or insource if necessary—the capacity to conduct most aspects of offensive cyber operations. Second, because the data analytics market is made up of many nontraditional defense contractors, it is imperative that the DOD and other agencies look beyond established suppliers to ensure they procure services from the most qualified companies. The DCGS-A2 case demonstrates that agencies may have difficulty evaluating the relative capabilities of companies in the analytics field, while also favoring established defense contractors over new entrants to the marketplace. If the national security community seeks access to the best analytics and machine learning technologies, it must be more open to working with nontraditional suppliers. The CIA and DOD have recently made efforts to access technologies emerging in start-up businesses through initiatives such as In-Q-Tel and the Defense Innovation Unit (DIU); however, major obstacles still exist for commercial firms seeking to work in the defense industry.[116]

In conclusion, as technology becomes increasingly central to national security, corporations are likely to assume a more central role in military and intelligence operations. While cooperation with the private sector contributes to American defense capabilities, the DOD and the intelligence community must continue to implement rigorous procurement practices to ensure they hire the most capable service providers and monitor contractors' performances meticulously. This will prove challenging as new suppliers of cybersecurity and other technology services seek to enter the rapidly growing United States defense market.[117] To successfully navigate future outsourcing challenges, the national security community will need to balance the entrance of major commercial technology firms like Amazon and Microsoft with agencies' existing relationships with traditional defense contractors such as Raytheon and Northrop Grumman. Additionally, the DOD should make further efforts to access cutting-edge innovations emerging from smaller technology firms while overcoming any lingering anti-defense bias that exists in some commercial circles. Historically, the partnership between the United States' dynamic businesses and the national security community has been a strategic asset. To make sure this pattern carries on in cyberspace and beyond, the DOD and the intelligence community should continue to innovate their outsourcing practices while carefully monitoring and evaluating the work defense contractors perform. SSQ

Charles W. Mahoney

Dr. Mahoney is an associate professor in the Department of Political Science at California State University, Long Beach. He holds a PhD from UCLA. His research on international security, foreign policy, and defense outsourcing has been published in numerous scholarly journals.

Notes

1. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, 2018), https://dod.defense.gov/.

2. Kristen E. Eichensehr, "Public-Private Cybersecurity," *Texas Law Review* 95, no. 3 (2017): 467–538, http://texaslawreview.org/. Cybersecurity partnerships between governments and the private sector also may occur on an ad hoc basis.

[3] Exceptions include Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2018), 71–80; Martin Libicki, David Senty, and Julia Pollack, *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND, 2014), https://www.rand.org/; and Irving 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), 379–401.

[4] Eugene Gholz and Harvey Sapolsky, "Restructuring the U.S. Defense Industry," *International Security* 24, no. 3 (1999): 5–51, https://www.belfercenter.org/; P. W. Singer, *Corporate Warriors*: *The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2003); Deborah Avant, *The Market for Force: The Consequences of Privatizing Security* (Cambridge, MA: Cambridge University Press, 2005); and Sean McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order* (New York: Oxford University Press, 2014).

[5] Eugene Gholz and Harvey M. Sapolsky, "The Very Healthy US Defense Innovation System," UC San Diego Study of Information and Technology in China (SITC) Research Briefs, Series 10: Defense Innovation, 2018-5, https://escholarship.org/.

[6] Rhys McCormick, *Defense Acquisition Trends 2019: Topline DoD Trends* (Washington, D.C.: Center for Strategic & International Studies, 2019), https://www.csis.org/; 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), https://fas.org/; 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); and Laura A. Dickinson, *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs* (New Haven, CT: Yale University Press, 2011).

[7] Schwartz, Sargent, and Mann, *Defense Acquisitions*, 1.

[8] Govini, *Federal Cybersecurity: FY18 Standard Market Taxonomy of Unclassified Spending* (Alexandria, VA: Govini, 2017), 1. Govini is a data analysis company that performs work for various United States defense agencies. The data the firm receives and analyzes comes directly from government departments and agencies.

[9] The DOD makes a distinction between defensive cyber operations and securing the Department of Defense Information Network (DODIN). For the purposes of conceptual parsimony, this inquiry merges these two activities.

[10] It can be difficult to distinguish offensive and defensive operations in cyberspace. For more on this topic, see Eric Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyber Space," *Security Studies* 24, no. 2 (2015): 316–48.

[11] Joint Publication (JP) 3-12, *Cyberspace Operations*, 8 June 2018, II-5, https://www.jcs.mil/.

[12] JP 3-12, II-5.

[13] Govini, *Federal Cybersecurity*, 2.

[14] Govini, 2.

[15] Booz Allen Hamilton, "Cyber Fusion Center: Next Gen Security Operations," accessed January 2021, https://www.boozallen.com/.

[16] General Dynamics, corporate website, accessed January 2021, https://www.gdit.com/.

17. Software engineers often prefer working in the private sector due to more lucrative salaries and greater work flexibility. This has resulted in staffing difficulty at CYBERCOM. See Mark Pomerleau, "The Army's New Multi-Domain Units Are Understaffed," *Fifth Domain*, 15 August 2019, https://www.fifthdomain.com/.

18. Patrick Howell O'Neill, "After a Long Fight, Raytheon Wins $1 Billion Cybersecurity Contract with Homeland Security," *Cyberscoop*, 19 June 2017, https://www.cyberscoop.com/.

19. Mark Pomerleau, "Cyber Command Awards $54M Contract for Cyber Carrier," *Fifth Domain*, 29 October 2018, https://www.fifthdomain.com/.

20. For more on the difficulty the national security community has experienced working with technology firms, see Amy Zegart and Michael Morrell, "Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail," *Foreign Affairs* 98, no. 3 (May/June 2019): 85–96, https://www.foreignaffairs.com/.

21. Sharon Weinberger, "The Everything War," *MIT Technology Review* 122, no. 6 (2019): 28, https://wp.technologyreview.com/.

22. Weinberger, 28.

23. Kate Conger, "Judge Halts Work on Microsoft's JEDI Contract, A Victory for Amazon," *The New York Times*, 13 February 2020, https://www.nytimes.com/. In October 2019, the DOD awarded the JEDI contract to Microsoft; however, Amazon challenged the award, and in February 2020, a federal judge halted all work on JEDI pending legal resolution of Amazon's protest.

24. Conger, "Judge Halts Work."

25. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 90–113, https://www.airuniversity.af.edu/.

26. JP 3-12, *Cyberspace Operations*, II-5. The Joint Chiefs of Staff distinguish between blue cyberspace controlled by the DOD and its partners and red cyberspace—which is cyberspace owned or controlled by an adversary. Gray cyberspace refers to all cyberspace that does not meet the description of blue or red cyberspace.

27. Govini, *Federal Cybersecurity*, 1.

28. Lachow and Grossman, "Cyberwar."

29. Justin Lynch, "Security Companies See Opportunity in Trump's New Cyber Plan," *Fifth Domain*, 26 September 2018, https://www.fifthdomain.com/.

30. James Bach, "SAIC Sees Opportunity in Feds 'Offensive Cyber' Efforts," *Washington Business Journal*, 25 May 2016, https://www.bizjournals.com/.

31. James Bach, "Leidos CEO Roger Krone Confirms That Company Does 'Offensive Cyber' for Feds," *Washington Business Journal*, 5 May 2016, https://www.bizjournals.com/.

32. ManTech, corporate website, accessed December 2020, https://www.mantech.com/.

33. CACI, corporate website, accessed December 2020, http://investor.caci.com/.

34. Bach, "SAIC Sees Opportunity"; and SAIC, corporate website, accessed December 2020, https://jobs.saic.com/jobs/.

35. Kate M. Manuel, *Definitions of "Inherently Governmental Function" in Federal Procurement Law and Guidance* (Washington, D.C.: Congressional Research Service, 2014), https://digital.library.unt.edu/.

36. For more 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, D.C.: Congressional Research Service, 2009), https://fas.org/.

37. Renée De Nevers, "Private Security Companies and the Laws of War," *Security Dialogue* 40, no. 2 (April 2009): 169–90, https://doi.org/10.1177/0967010609103076.

38. Manuel, *Definitions of "Inherently Governmental Function,"* 3.

39. John S. Hurley, "Enabling Successful Artificial Intelligence Implementation in the Department of Defense," *Journal of Information Warfare* 17, no. 2 (2018): 65–82, https://www.jstor.org/stable/26633155?seq=1.

40. Zak Doffman, "Russia Unleashes New Weapons in Its Cyberattack Testing Ground," *Forbes*, 5 February 2020, https://www.forbes.com/.

41. Office of the Director of National Intelligence, *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, D.C.: Office of the Director of National Intelligence, 2019), https://www.dni.gov/.

42. Govini, *Federal Cybersecurity*, 16. Govini's data on analytics tracks spending on cyber related analytics contracts and not on all federal spending on AI and machine learning technologies, which is likely much higher.

43. Govini, 16.

44. Govini, 16.

45. Charles W. Mahoney, "Acquire or Expire: Publicly Traded Defense Contractors, Financial Markets, and Consolidation in the U.S. Defense Industry," *Defence and Peace Economics*, 2019, https://doi.org/10.1080/10242694.2019.1667216.

46. For more on the relationship between Palantir and In-Q-Tel, see Peter Waldman, Lizette Chapman, and Jordan Robertson, "Palantir Knows Everything About You," *Bloomberg Businessweek*, 19 April 2018, https://www.bloomberg.com/; and Murad Ahmed, "Palantir Goes from CIA Funded Start-Up to Big Business," *Financial Times*, 24 June 2015.

47. Ken Dilanian, "US Special Operations Forces are Clamoring to Use Software from Silicon Valley Company Palantir," *Business Insider*, 26 March 2015, https://www.businessinsider.com/; and Palantir, "Fielding an Advanced Analytic Capability in a Warzone," accessed December 2020, https://www.palantir.com/.

48. Kate Fazzini and Amanda Macias, "Peter Thiel's Company Palantir Just Won a Major Pentagon Contract, Beating Out Traditional Military Vendors," *CNBC*, 27 March 2019, https://www.cnbc.com/.

49. Palantir, corporate website, accessed January 2021, https://www.palantir.com/.

50. Palantir, corporate website.

51. Aaron Gregg and Douglas MacMillan, "Palantir Goes Public at $10 Dollars per Share," *The Washington Post*, 1 October 2020, https://www.washingtonpost.com/.

52. Lindsey R. Sheppard, *Artificial Intelligence and National Security: The Importance of the AI Ecosystem* (Washington, DC: Center for Strategic and International Studies, 2018), https://www.csis.org/.

53. Graham Allison, "Is China Beating America to AI Supremacy?," *The National Interest*, 22 December 2019, https://nationalinterest.org/.

54. James Vincent, "Putin Says the Nation That Leads in AI 'Will be the Ruler of the World,'" *The Verge*, 4 September 2017, https://www.theverge.com/.

55. All organizations—within and outside government—must choose what goods and services they will produce internally and what inputs and operations they will outsource. Even organizations with high levels of vertical integration typically outsource important aspects of their operations. This "make or buy" decision is foundational to the field of transaction cost economics. For more on this body of work, see Ronald Coase, "The Nature of

the Firm," *Economica* 4, no. 16 (1937): 386–405, https://doi.org/10.1111/j.1468-0335.1937.tb00002.x; Ronald Coase, "The Problem of Social Cost." *Journal of Law and Economics* 3 (1960): 1–44, https://www.law.uchicago.edu/; and Oliver Williamson, "The Economics of Organization: The Transaction Cost Approach," *The American Journal of Sociology* 87, no. 3 (November 1981): 548–77, https://doi.org/10.1086/227496.

56. Robert J. David, "A Systematic Assessment of the Empirical Support for Transaction Cost Economics," *Strategic Management Journal* 25, no. 1 (2004): 39–58, https://doi.org/10.1002/smj.359.

57. For a discussion of transaction cost economics and its application to public bureaucracies, see Oliver E. Williamson, "Public Bureaucracies: A Transaction Cost Economics Approach," *The Journal of Law, Economics, & Organization* 15, no. 1 (April 1999): 306–42, https://www.jstor.org/stable/3554953?seq=1.

58. Oliver E. Williamson, "Transaction Cost Economics: How It Works, Where It Is Headed," *De Economist* 146, no. 1 (1998): 23–58, https://doi.org/10.1023/A:1003263908567.

59. Peter Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, MA: Harvard University Press, 2003), 74.

60. James Cockayne, "Make or Buy? Principal-Agent Theory and the Regulation of Private Military Companies," in *From Mercenaries to Markets: The Rise and Regulation of Private Military Companies*, eds. Simon Chesterman and Chia Lehnardt (Oxford: Oxford University Press, 2007), 197.

61. The term "asset specificity" was coined by Oliver E. Williamson. For more on the topic see Oliver E. Williamson, *The Economic Institutions of Capitalism* (New York: Free Press, 1985).

62. Chris Lonsdale, "Locked-In to Supplier Dominance: On the Dangers of Asset Specificity for the Outsourcing Decision," *Journal of Supply Chain Management* 37, no. 2 (Spring 2001): 22–27, *Gale Academic OneFile*, accessed 22 January 2021, https://go.gale.com/.

63. Other types of asset specificity include site asset specificity, temporal asset specificity, and brand asset specificity. For more on conceptualization of asset specificity, see Glauco De Vita, Arafet Tekaya, and Catherine L. Wang, "The Many Faces of Asset Specificity: A Critical Review of Key Theoretical Perspectives," *International Journal of Management Reviews* 13, no. 4 (2011): 329–48, https://doi.org/10.1111/j.1468-2370.2010.00294.x.

64. Gordon Walker and David Webber, "A Transaction Cost Approach to Make-or-Buy Decisions," *Administrative Science Quarterly* 29, no. 3 (1984): 373–91, https://doi.org/10.2307/2393030.

65. Paul L. Joskow, "Asset Specificity and the Structure of Vertical Relationships: Empirical Evidence," *Journal of Law, Economics, and Organization* 4, no. 1 (1988): 95–177, http://www.jstor.org/stable/765016.

66. De Vita, Tekaya, and Wang, "The Many Faces of Asset Specificity," 329–48.

67. 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, https://doi.org/10.1080/09636412.2017.1243912.

68. Keith Hartley, "The Arms Industry, Procurement and Industrial Policies," in *Handbook of Defense Economics: Defense in a Globalized World*, eds. Todd Sandler and Keith Hartley (New York: North Holland, 2007), 1161.

69. Todd Sandler and Keith Hartley, *The Economics of Defense* (New York: Cambridge University Press, 1995), 127–28.

70. Sandler and Hartley, 127–28.

71. Raymond Franck and Francois Melese, "Defense Acquisition: New Insights from Transaction Cost Economics," *Defense & Security Analysis* 24, no. 2 (2008): 107–28, https://doi.org/10.1080/14751790802124931.

72. J. Eric Fredland, "Outsourcing Military Force: A Transactions Cost Perspective on the Role of Military Companies," *Defence & Peace Economics* 15, no. 3 (2004): 205–19.

73. Maurer, *Cyber Mercenaries*, 71.

74. The CFAA was first enacted in 1986 and last amended in 2008. See Cornell Law School, Legal Information Institute, 18 U.S. Code § 1030 – Fraud and related activity in connection with computers, https://www.law.cornell.edu/.

75. This type of implied counterfactual claim is common in social science research and relates to the "fundamental problem of causal inference," which argues that there will always be uncertainty underlying causal claims in the social sciences because history cannot be rerun in order to assess the precise effect the presence or absence of a specific independent variable has on an observed outcome. For more on this topic, see Paul W. Holland, "Statistics and Causal Inference," *Journal of the American Statistical Association* 81, no. 396 (1986): 945–60, https://doi.org/10.1080/01621459.1986.10478354; Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry: Scientific Inquiry in Qualitative Research* (Princeton, NJ: Princeton University Press, 1994), 76–82; and James D. Fearon, "Counterfactuals and Hypotheses Testing in Political Science," *World Politics* 43, no. 2 (1991): 169–95, https://doi.org/10.2307/2010470.

76. While the DOD and other government departments can try and avoid adverse selection through R&D projects and competitive prototyping, it is not possible to carry out controlled comparisons for all the major procurement RFPs government agencies issue on an annual basis.

77. The GAO has formally handled the federal bid protest process since 1984 when Congress passed the Competition in Contracting Act with the goal of increasing transparency in the government's contracting process. For more on the bid protest process, see GAO's website, https://www.gao.gov/legal/bid-protests.

78. Mark V. Arena et al., *Assessing Bid Protests of U.S. Department of Defense Procurements: Identifying Issues, Trends, and Drivers* (Santa Monica, CA: RAND, 2018), 9, https://www.rand.org/.

79. Arena et al., 9.

80. Arena et al., xiii–xv. A recent RAND study hypothesized that small companies are more likely to file bid protests because the revenue they stand to lose by not winning an award can pose a serious threat to their continued business operations.

81. Many defense contractors advertise for job openings in the field of offensive cyber operations; however, to date the only publicly awarded contract generally believed to include offensive cyber operations is USCYBERCOM's $460 million 2016 operations support contract, which was awarded to six different corporations. See Aaron Boyd, "CYBERCOM Awards Spots on New $460 Million Cyber Operations Contract," *Federal Times*, 23 May 2016, https://www.federaltimes.com/.

82. For more on exploratory case studies, see John Gerring, *Case Study Research: Principles and Practices* (New York: Cambridge University Press, 2017), 65–83.

83. United States Government Accountability Office (US GAO), *Northrop Grumman Systems Corporation; B-412278.7, B-412278.8* (Washington, D.C.: Comptroller General of the United States, 4 October 2017), https://www.gao.gov/.

84. US GAO, *Northrop Grumman Systems Corporation*.

85. The NCPS is operationally known as the "EINSTEIN set of capabilities" and is often simply referred to as EINSTEIN in government and press publications referencing NCPS.

86. US GAO, *Northrop Grumman Systems Corporation*, 3.

87. Jason Miller, "DHS Awards $1 Billion Cyber Contract to Protect Agency Networks," *Federal News Network*, 23 September 2015, https://federalnewsnetwork.com/.

88. US GAO, *Northrop Grumman Systems Corporation*, 17.

89. US GAO, 17.

90. US GAO, 17.

91. US GAO, 18.

92. US GAO, 18.

93. US GAO, 18.

94. US GAO, 21.

95. The United States Court of Federal Claims, *Palantir USG Inc. v. United States*, No. 16-784C, 3 November 2016, 3, https://ecf.cofc.uscourts.gov/.

96. United States Government Accountability Office, *Palantir USG, Inc.; B-412746* (Washington, D.C.: Comptroller General of the United States, 2016), https://www.gao.gov/.

97. US GAO, *Palantir USG*.

98. Raytheon, "United States Army Analysis and Control Element (ACE) Block II, Distributed Common Ground System—Army (DCGS-A)," case study, 2014, https://www.raytheon.com/; and Lockheed Martin, "U.S. Army Testing Lockheed Martin's Upgrades to Battlefield Intelligence Enterprise," 14 October 2014, https://news.lockheedmartin.com/.

99. Jen Judson, " 'Powerful Tool' but 'Requires Extensive Training': Soldiers Find DCGS-A Hard to Use as Difficulties Hinder Operations," *Inside the Army* 26, no. 6 (2014): 8–9, http://www.jstor.org/stable/24836007.

100. Greg Slabodkin, "Distributed Common Ground System Comes under Fire," *Defense Systems*, 1 October 2012, https://defensesystems.com/.

101. Rowan Scarborough, "Problems with Army's Battlefield Intel System Unresolved after Two Years," *The Washington Times*, 1 May 2014, https://www.washingtontimes.com/.

102. The United States Court of Federal Claims, *Palantir USG Inc. v. United States*, 4.

103. Before the Army issued the DCGS-A2 RFP, it conducted a market research review and determined that no commercially available products were suitable for the DCGS platform.

104. US GAO, *Palantir USG, Inc.; B-412746*.

105. US GAO, *Palantir USG, Inc.; B-412746*.

106. Sean Lyngaas, "Palantir to Sue Army over DCGS," *Federal Computer Week*, 20 June 2016, https://fcw.com/articles/.

107. The United States Court of Federal Claims, *Palantir USG Inc. v. United States*, 93.

108. The United States Court of Federal Claims, 16.

109. The United States Court of Federal Claims, 104.

110. The United States Court of Federal Claims, 94.

111. The United States Court of Federal Claims, 96.

112. Nick Wakeman, "Palantir, Raytheon to Battle Under $876m Army DCGS-A Contract," *Washington Technology*, *WT Business Beat* (blog), 12 March 2018, https://washingtontechnology.com/.

113. Shane Harris, "Palantir Wins Competition to Build Army Intelligence System," *Washington Post*, 26 March 2019, https://www.washingtonpost.com/.

114. Jackson Barnett, "Palantir, BAE Score $823 Million Contract to Modernize Army's Distributed Common Ground System," *Fedscoop,* 26 February 2020, https://www.fedscoop.com/.

115. Aaron Gregg, "Palantir Seals Its First Major U.S. Navy Deal as Raytheon Is Passed Over," *The Washington Post*, 5 March 2020, https://www.washingtonpost.com/.

116. In 2016, the Pentagon announced the formation of the Defense Innovation Unit (DIU), a DOD organization tasked with helping the military gain access to cutting-edge technological innovation in the private sector. For more on the DIU see Aaron Metha, "Former Symantec Boss Takes Over at Defense Innovation Unit," *Defense News*, 24 September 2018, https://www.defensenews.com/.

117. DOD outlays on defense contractors totaled $402 billion in 2019. See Daniel Snyder, "Federal Contract Spending: Five Trends in Five Charts," *Bloomberg Government*, 6 January 2020, https://about.bgov.com/.

Disclaimer and Copyright

The views and opinions in *SSQ* are those of the authors and are not officially sanctioned by any agency or department of the US government. This document and trademarks(s) contained herein are protected by law and provided for noncommercial use only. Any reproduction is subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the *SSQ* editor for assistance: strategicstudiesquarterly@au.af.edu.