CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

JUNE 2020

Partnership for Countering Influence Operations

Collaborative Models for Understanding Influence Operations: Lessons From Defense Research

Jacob N. Shapiro, Michelle P. Nedashkovskaya, and Jan G. Oledan

Collaborative Models for Understanding Influence Operations: Lessons From Defense Research

Jacob N. Shapiro, Michelle P. Nedashkovskaya, and Jan G. Oledan

Carnegie's Partnership for Countering Influence Operations (PCIO) is grateful for funding provided by the William and Flora Hewlett Foundation, Craig Newmark Philanthropies, Facebook, Twitter, and WhatsApp. PCIO is wholly and solely responsible for the contents of its products, written or otherwise. We welcome conversations with new donors. All donations are subject to Carnegie's donor policy review. We do not allow donors prior approval of drafts, influence on selection of project participants, or any influence over the findings and recommendations of work they may support.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Introduction

Social media has proven itself an essential tool for catalyzing political activism and social change in the United States and around the world.[1] Yet the very features that make it so useful to those seeking to advance the greater good—scalability, mobility, and low costs to entry—also make it prone to manipulation by malign actors who use it to perform influence operations and spread divisive rhetoric. These bad actors looking to sway public opinion include both fringe groups and well-funded, highly staffed government institutions, and they have been prolific in recent years.[2] This new type of statecraft is but one example of the wide-ranging impacts social media have on society, a topic that demands greater research and long-term institutional investments.

A key barrier to expanding the knowledge base on influence operations is getting credible, reproducible, scientific research done with highly sensitive data. This challenge can in principle be addressed either by company staff (insourcing) or by outside academics (outsourcing), but both routes have limitations.

Despite the expressed desire of and clear incentives for social networks and internet platforms to support better research, insourcing such research is difficult. Common challenges include: getting personnel and budgets for research that lacks an obvious pathway to product, managing data privacy concerns, establishing the credibility of studies, grappling with the difficulty of starting projects that might reflect poorly on platforms, and overcoming the limitations on work that crosses platform boundaries because of a widespread reluctance among social media companies to share data with competitors. Recruiting top-tier talent can also be a challenge, given that many researchers are reluctant to work at such companies for fear they will not be able to publish or that their independence will be questioned.[3] Because of such obstacles, companies are doing little internal research on long-term, noncommercial issues, at least relative to the massive volumes of data produced every second of every day.[4]

Outsourcing research by sharing data with academics introduces a different set of challenges. Technology companies face a wide range of legal and reputational risks when they allow outsiders to work with individual user account data. Previous attempts to circumvent these obstacles by outsourcing research have also fallen well short of expectations. To cite one example, in 2018, Facebook and a consortium of foundations along with scholars from Harvard, Stanford, and other universities established Social Science One. The organization's Election Research Commission followed a model in which a group of scholars worked with Facebook to identify data that could be safely anonymized and then released to researchers—a task that turned out to be much harder to operationalize than anticipated.[5] Efforts to establish data-sharing institutions analogous to the U.S. government's Federal

Statistical Research Data Centers (RDCs) have not yet borne fruit for the wider academic community (the Stanford Internet Observatory, for example).[6] And while ad hoc collaborations have solved some of the challenges discussed above, they are typically based on personal relationships that do not scale.[7]

Both researchers and industry actors (a shorthand term for social media companies and internet platforms) need new models for thinking about how to build durable organizations that can draw on a wide range of expertise, pivot to new problems, remain stable enough to attract top talent, and work flexibly with a plethora of highly sensitive information. To maximize knowledge development, these organizations need to address incentive-related issues at multiple stages in the research process—from conceptualizing to resourcing to data sharing to publishing. Such organizations also need to enable cross-platform work in ways that no existing system does.

The long-running relationship between academic researchers and the U.S. defense community provides several institutional models that can serve as inspiration for developing new solutions to fill this gap. These rich forms of ongoing collaboration almost all sit somewhere between the platonic open science ideal on the one hand and proprietary inhouse research on the other. They involve compromises and the clever use of contractual, financial, and reputational mechanisms to connect skilled researchers with hard problems while giving them the resources necessary to make progress. These models could shape how industry actors think about and seek to catalyze research on issues ranging from combating malign influence operations to mitigating the psychological costs of distraction.

Taken as a whole, the defense research ecosystem has largely solved a range of tasks that need to be addressed in industry-academia collaboration (or at least their defense equivalents). Three stand out as especially critical in light of recent experiences:

Task 1: maintaining credibility and engaging external researchers;
Task 2: safeguarding data while enabling cross-platform research; and
Task 3: overcoming structural barriers, including:

- insufficient decision cycles at the top,
- reluctance to study certain topics,
- product-oriented culture,
- and short-term focus.[8]

Throughout this paper, these three tasks serve as a framework for evaluating different initiatives and the issues they do, or do not, solve. The remainder of the paper explores lessons from the rich history of defense-academia collaboration, providing examples that could inform thinking about how to better support research on online influence operations, among other topics related to emerging technologies. The first section briefly discusses the limitations of existing models for addressing the three tasks outlined above, covering both the challenges of insourcing and the difficulties of outsourcing. Next, the paper examines formal and informal models of collaboration from other fields, primarily defense and intelligence but also labor economics. These models are familiar to some but are not well-known in the wider community working on influence operations. The final section concludes with a discussion of the benefits of intermediate organizations and five concrete principles for setting them up.

Limitations of Existing Models

In recent years, there have been several efforts to better understand how social media can be used for malign purposes. The major social media platforms all have established internal research groups, several think tanks have created research arms, and various academics have developed a number of models in parallel. Collectively, these institutions have cultivated a wide range of valuable knowledge, but they have also fallen short in important ways.

Challenges of Insourcing

One seemingly clear solution to the challenge of studying the impact of social media on society is for firms to undertake the work themselves by insourcing. Unfortunately, while social media and internet platforms obviously must play a critical role in these investigations, they face specific constraints that hamper their ability to drive scientific research on multiyear time frames.[9]

Industry actors face real challenges producing credible research (see task 1 above), as evidenced by the lukewarm public reaction to large platforms' significant steps to increase their internal capacities for combating online influence efforts. Facebook, for example, has hired hundreds of staff and invested in a range of new technologies to help target what it calls "coordinated inauthentic behavior" across its products.[10] Google has been supporting more effective journalism through its Google News Initiative while working on proactive strategies for keeping disinformation out of search results.[11] And Twitter has been shutting down accounts associated with online manipulation and

publishing extensive data to contribute to research on state-sponsored influence operations.[12] Despite these recent initiatives,[13] social media companies continue to come under fire for their failure to quell inauthentic behavior.[14]

Why is that the case? Part of the answer is surely the fallout from recent scandals, which have shaken public trust in industry actors, exacerbating systemic obstacles to credible research.[15] Trust in Facebook, for example, reportedly declined by 66 percent in the wake of the major 2018 privacy scandal involving the use of the company's data by Cambridge Analytica.[16] Since then, the platform has also come under fire for releasing a Facebook Research app that granted the company expansive access to users' mobile devices.[17] Such scandals have dramatically impacted public perceptions of industry actors, thereby magnifying concerns regarding the independence and ethics of internal research.[18] They also reinforce companies' history of incomplete disclosures, which raises questions about their willingness to publish findings that would reflect poorly on their impact or policies.[19] That history also elevates concerns about file-drawer bias—the distortion of overall knowledge when null results are less likely to be published.[20] Because companies have strong financial incentives to suppress unfavorable research findings, purely insourced research will likely always be met with suspicion.

The core of task 2, safeguarding data, is relatively straightforward for purely internal research. But the second half of this task (enabling cross-platform research) makes maintaining security much harder.[21] By definition, cross-platform work cannot be purely insourced. This poses a real challenge because sophisticated social media manipulators operate across many platforms at once, so the ability of any single company to identify and target them is inherently limited.

Moreover, fully understanding the structure and impacts of influence operations will likely require working with information from smaller platforms that typically have limited analytical resources. Tracking the profiles and activities of bad actors across platforms is important for understanding how influence campaigns are managed, but researchers cannot reliably assess that impact if they systematically lack exposure to data from smaller platforms. Yet many such firms lack the resources to make the kinds of investments in identifying online manipulation that larger companies have done. Insourcing alone simply cannot suffice, at least not without dramatic improvements in cross-platform information sharing.

Finally, industry actors have not been able to overcome the range of structural barriers that task 3 entails. Even when relevant actors intend to do so, many of their efforts have been stymied or have taken far longer than expected because they require senior leaders' attention for coordination across different divisions. Projects expected to yield findings unfavorable to firms (that are therefore unpopular with some senior executives) are put off or go under-resourced. And getting research plans

approved is often complicated by the frequent internal reorganizations endemic to most social media platforms. Most of these companies have grown amid a period of extremely rapid change, leading to a culture of frequent personnel turnover and reorganization.[22] This makes executing multiyear research projects extremely difficult as each leadership change or restructuring necessitates another round of coalition building for such projects.[23] High turnover also creates obstacles related to talent recruitment. People with the skills to execute the most challenging basic research typically want to work in places where they can focus on one problem set for a long period of time.

In some ways, the most significant structural barrier relates to the short-term, product-focused culture prevalent at most social media companies.[24] The connection between such research inquiries and companies' products is often unclear at the start of basic research projects (indeed the outcome is by definition unknown—otherwise it would not be research), so they are a hard sell at many companies. That uncertainty also makes it hard to defend personnel and budgetary allocations when unexpected product-related issues come up (if, for example, a major software release has unanticipated consequences for other products and requires reallocating engineering resources). These challenges are exacerbated when projects require coordination across multiple divisions. In addition to a strong product-oriented culture, most social media platforms also tend to focus on the short term, especially on results for the next quarter, half or year. Though characteristic of many dynamic, for-profit companies, this feature makes it hard to execute projects that last several years, as many social science projects often do.

Between the myriad challenges associated with the lack of trust in technology companies, data privacy concerns, limitations on cross-platform research, and structural barriers, insourcing alone cannot solve the research gap. This leaves several unanswered questions that are important to democracy: what effect (if any) do influence operations have on audience decisionmaking? Do existing countermeasures on influence operations work? And could platforms' content moderation policies inadvertently stifle political speech by U.S. citizens? Addressing such inquiries will require innovative approaches that go beyond insourcing.

Difficulties of Outsourcing

Outsourcing poses a different set of challenges. Industry actors working with outside organizations have achieved some notable successes. For example, the Digital Forensics Research Laboratory, which is supported by Facebook information sharing, produces some of the richest publicly available data sources on troll tactics, techniques, and procedures. Unfortunately, more often than not, data privacy concerns stymie such forms of collaboration.

The Social Science One initiative exemplifies these challenges.[25] Social Science One was specifically designed to credibly engage outside researchers (task 1) through a three-stage process. First, a distinguished academic commission, the so-called Election Research Commission, would serve as a trusted third party, understanding the needs of the academic community while enjoying full access to the company's proprietary data so that it could identify data that would serve scholarly goals. Then the board and companies (initially Facebook) work to anonymize the data to preserve user privacy, and lastly, outside academics whose research plans pass a peer review process gain data access and the ability to publish their findings without the company's prior approval, a measure enacted to support research independence.[26] Impartiality concerns would also be allayed by funding the initiative with support from an ideologically diverse group of charities. This approach was designed to enable high-credibility research while protecting user privacy as well as firms' closely guarded trade secrets.

While Social Science One made admirable strides toward surmounting the issues inherent to inhouse approaches—and while it supported important data releases and promising studies—it also faced a host of unanticipated challenges that ultimately prevented it from achieving many of its stated goals. Most critically, the group's leadership underestimated the difficulty of addressing privacy concerns associated with releasing the initiative's first data set.[27] Facebook was unable to give researchers the promised fine-grained data because large-scale anonymization proved technically and legally more challenging than anticipated. The limited data that Social Science One could provide paled in comparison to what had been promised, leading some funders to pull support from the initiative.[28]

Ultimately, operational hurdles prevented Social Science One from addressing task 2 and task 3. It was not able to safeguard data in the manner needed to get the most out of the academic researchers. It also did not address many of the long-term structural barriers that go beyond data access (nor was it intended to do so, except by serving as a demonstration of one possible approach). Social Science One required a large, bespoke, one-off effort at data anonymization that advanced the state of the art on that topic, but it did not create a set of durable organizational processes.

Of course, the litany of data-sharing problems that can stymie research extend well beyond anonymization. Even highly competent companies can have horribly messy data. Firms often have not standardized data across products, compounding the challenges of sharing and making sense of it.[29] And documentation is usually sparse and incomplete compared to what academic researchers need. Resolving those problems within firms before data is shared can require costly engineering efforts as well as collaboration across business units. These additional complications mean that researchers need to develop deep, long-term, collaborative relationships to be able to address the third task. Otherwise they will have a hard time knowing what kinds of data they can, or cannot, expect to have for their research, nor what to make of the data that is released.

The failures of outsourcing up to this point should not stop the search for institutional frameworks that would allow for data sharing by industry actors. But the most prominent efforts that firms and academic researchers have undertaken are corner solutions, either purely insourced or focused on pushing data out in an open science framework, two approaches that both will likely continue to falter in important ways. That state of affairs should push industry and the research community toward innovative institutional solutions.

Models From the Defense and Security Fields

The long history of cooperation between academic researchers and the U.S. government in several areas, including defense and security, provides a rich set of examples for how to address the three key tasks identified in the introduction:

Task 1: maintaining credibility and engaging external researchers;
Task 2: safeguarding data while enabling cross-platform research; and
Task 3: overcoming structural barriers.

This section first highlights the role of informal mechanisms in fostering productive relationships between academic and defense institutions. It then reviews a number of formal organizations that have facilitated research projects that could neither be fully insourced by the government nor outsourced to academic institutions through competitive research grants.

Informal Mechanisms

Personal interactions between researchers and practitioners have long been a key part of the research base underpinning U.S. defense policy. Such relationships provide scholars with the deep knowledge of often highly sensitive national security matters necessary to identify which questions can be answered with the academic's craft.

Foundational work on nuclear strategy through engagement by Nobel laureates Thomas Schelling and Albert Wohlstetter, for example, was deeply informed by engaging with the operational nuclear weapons community while at the RAND Corporation.[30] Similarly, critical work by Scott Sagan on the inherent organizational limits to nuclear weapons safety drew on his time as a Council on Foreign Relations (CFR) International Affairs Fellow working for the Joint Chiefs of Staff and later as a consultant in the same office.[31] New research by Caitlin Talmadge on the potential for nuclear escalation in conventional wars draws on dozens of interviews conducted with current and former

officials, many of whom were willing to speak on the basis of interpersonal ties formed during Talmadge's time as a CFR Stanton Nuclear Security Fellow, as well as her interlocutors' tours as government fellows at think tanks and universities in Washington, DC.

To be sure, there are supporting institutions that nurture such long-term interpersonal ties. The most notable on the academic side is the CFR International Affairs Fellowship (IAF), which has funded approximately 600 fellows since 1967. IAF places mid-career foreign policy professionals, including academics, in new roles to expose the public sector to scholars and vice versa. Some of the leading academic research on the long-term implications of drones and artificial intelligence, for example, would not have happened absent connections and background knowledge that Michael C. Horowitz developed during his IAF stint.[32] On the military/defense side, the Army War College Military Education Level 1 (MEL-1) Fellows program is one of many funded educational opportunities through which active-duty personnel can build relationships with the research community. MEL-1 fellows spend a year at universities such as Harvard, Princeton, and Stanford or think tanks such as the Brookings Institution.[33] By giving researchers and their colleagues in the defense policy community opportunities to build trust and establish shared knowledge, these programs help lay the groundwork for data sharing and for overcoming structural barriers (task 3).

Informal relationships are also at the core of the last decade's flourishing body of research on insurgencies and irregular warfare. One of the authors of this paper, Shapiro, has been part of that effort as co-director of the Empirical Studies of Conflict Project (ESOC),[34] a multi-university consortium based out of Princeton University.[35] Since 2009, ESOC has supported more than one hundred research papers in various ways, including: working to declassify and build data on combat incidents in Afghanistan, Iraq, Mexico, and the Philippines;[36] collaborating with U.S. Defense Department agencies to release internal documents from terrorist organizations and co-authoring research on them with scholars from the RAND Corporation;[37] developing qualitative data on program implementation in Iraq;[38] and working with multiple state-level bureaucracies to build information on contracting and development program execution in India.[39]

The ESOC experience highlights a number of principles for how academics can effectively engage with industry actors on highly sensitive topics.[40] First and foremost, regular, ongoing conversations are the best way to identify relevant data and research possibilities.[41] Researchers should get out there and understand their potential partners' problems before they ask for data. Such cooperative engagement helps researchers make more refined, precise requests—a critical consideration when partners have other responsibilities beyond supporting research, as they always do—and such back-and-forth conversations also create a set of shared concerns that help make partners more willing to spend time answering the kinds of unanticipated questions that come up any time one digs into new kinds of data.

Second, researchers should be flexible and expect projects to involve extensive iterations and phases of discovery. Many of the projects ESOC supported entailed multiple cycles through the process of identifying a question of interest to both sides, running initial analysis, figuring out that the data have various quirks and inconsistencies that must be understood to make sense of the results, providing initial results to the operational partner, asking follow-up questions, and revising the initial question. Building the kind of trust-based relationship that enables such iteration requires spending time in the operators' shoes. Asking operational partners to simply throw data over the wall rarely leads to good studies, whether those partners are government organizations or technology firms.

Third, researchers should be sensitive to the operational environment facing their partners.[42] As a practical matter, that means working to align cadences, questions, and interests. The key to aligning cadences is recognizing that large parts of scholars' early research process—scoping out new problems and organizing existing knowledge on a topic—can be exceptionally helpful to those building out tools on short time frames. By sharing what is learned in the preparations to do the work—for example, what the research literature does or does not say about a given policy's likely impact—researchers can earn substantial good will. When combined with breaking down big research questions into scientifically meaningful components that are relevant today, such informal consulting can help generate momentum for the data sharing needed to address larger questions.

Aligning on questions and interests requires translating basic research questions into terms that are meaningful to partners, whether they are staff officers in the military or product managers at technology companies. At a fundamental level, informal cooperation means horse-trading data access, support, and information for helping a given firm with research-driven insights. If scholars cannot make the answers meaningful, they have nothing to trade.

Finally, any informal collaboration requires patience with the logistics of securing data. There are often a wide range of legal questions surrounding access to data, whether through declassification of national security data or the release of sensitive company information. These can often be finessed—in the defense space that often means forgoing release of some potentially useful fields—but doing so requires a clear-eyed understanding of the rules.

Even when data can be released, many partners will not have key pieces of data in accessible formats. Production systems are rarely engineered for long-term storage, retrieval, and aggregation. Awareness of limitations is important as researchers making infeasible requests provide managers a good excuse to shut down potential studies. Once data are released, high-reliability research still requires a detailed understanding of the data-generating process. This can be a problem. Often the documenta-

tion needed for studies is not part of the operational data. Researchers need to be very motivated to share it because doing so often requires digging through old records, especially for studies that go back more than a year.

Interpersonal ties between the defense and academic communities have been key to furthering research on sensitive issues. Through iterative collaboration, researchers and practitioners have developed a rich understanding of each other's limitations while generating innovative ideas. Over time, industry-academia collaboration could likewise build trusted relationships to stimulate research. To do so, the communities could draw upon lessons from programs that have successfully fostered trust and informal ties in defense research.

Enabling Institutions

While developing trusted relationships is an art, there are institutions that have turned it into more of a science. The Laboratory for Analytic Sciences (LAS) at North Carolina State University, for example, has enabled wide-ranging examples of research collaboration between faculty and the intelligence community around sensitive security issues since its founding.[43] Government personnel spend multiyear tours at LAS where they work with university faculty and industry partners to address specific problems facing their home organizations. LAS has overcome several challenges in the process, such as surmounting structural and cultural differences across organizations, accommodating different approaches and jargon when problem solving, and fostering mutual trust so personnel work toward shared goals.[44]

LAS has been largely successful at developing a structured approach to encouraging collaboration among actors with vastly different institutional backgrounds. It employs several distinct annual workflows that offer predictability to faculty and students with a consistent approach to building teams that include academics, industry actors, and government officials. Over time, LAS has learned the characteristics of effective project leadership for its specific setting and has developed a pipeline to bring such people onto both the government and academic sides.[45] Because such extreme interdisciplinarity is not the norm for researchers or intelligence community personnel coming to work at LAS, the organization developed a dedicated collaboration team. That team advises leadership and facilitates research by suggesting process improvements to increase teamwork capacity across smaller units within the organization.[46]

The Defense Advanced Research Projects Agency (DARPA) is also a key enabler of informal ties because of how it staffs its R&D efforts. Established in 1958 within the U.S. Department of Defense to take on "high-risk, high-reward" R&D challenges, DARPA has solved a range of complex technical problems while creating connections among academics, government organizations, and

industry.[47] DARPA's innovation model combines ambitious goals with a system of temporary project teams comprised of interdisciplinary experts from industry, universities, and federal government organizations.[48]

DARPA projects are run by program managers, individuals recruited from the outside and tasked with developing, pitching, and then executing projects. DARPA program managers are term-limited, between three to five years, with an informal norm that one cannot do more than two tours in a career.[49] That structure encourages entry by people with innovative ideas and then pushes them out to other sectors with the knowledge and connections gained during their tenure.[50] Program managers join "to get something done, not build a career."[51] And if projects are not working, program managers can terminate them and reallocate funds to a new or existing project that demonstrates more promise.[52]

DARPA's innovative, risk-taking culture is sustained by unusual hiring and contracting flexibility compared to other Department of Defense agencies.[53] Importantly, these include the ability to hire experts from outside the government on short-term contracts.[54] Overall, DARPA's time-limited appointments and capacity to directly hire people with commercial or academic backgrounds into senior government positions encourages an exchange of ideas and perspectives that otherwise would never happen—a net benefit for all parties.

LAS and DARPA illustrate the broader principle that tackling research topics that cross organizational boundaries fosters long-term interdisciplinary relationships. They have solved many of the contracting and human-resources challenges involved in engaging external researchers and have overcome a range of structural barriers to insourcing research in the defense and intelligence communities.

Formal Mechanisms

There are two key formal mechanisms for collaboration between the federal government and academia when it comes to economic and defense issues involving sensitive data: RDCs and Federally Funded Research and Development Centers (FFRDCs).[55] This section looks at both these organizations for inspiration, focusing in particular on how they address the three key tasks identified in the introduction.

Federal Statistical Research Data Centers

RDCs enable individual researchers to work with highly sensitive, government-collected information, including individual-level survey data and firm-level responses to Bureau of Labor Statistics surveys.[56] These secure facilities are managed by the Census Bureau at twenty-nine different locations across the

United States, including at universities, Federal Reserve Bank branches, and a few other research institutions such as the National Bureau for Economic Research. To ensure data security, RDC researchers are required to obtain Census Bureau Special Sworn Status by passing a background check and swearing to protect respondent confidentiality for life.[57] These centers partner with more than fifty different research organizations, including universities, nonprofit research institutions, and government agencies. Thanks to their stringent security requirements, RDCs enable a wide variety of research using sensitive datasets such as firm-level surveys with identifying information.

RDC data have been used to study a wide range of topics over the years, including studies on the effect of fraudulent financial reporting on employees, the potential impact of adding citizenship questions to the 2020 census, and the ways in which having children shape employment dynamics for U.S. women.[58] These studies would be impossible without academic access to sensitive individual and firm data.

RDCs work for two reasons. First, by controlling the computing infrastructure on which analysis is conducted, the RDCs can ensure data do not leak. This way, firms are comfortable sharing sensitive data on Bureau of Labor Statistics surveys even though they know researchers may eventually work with the data. Second, researchers can plan projects before they go to RDCs because extensive data dictionaries are available, even when data themselves cannot be made public.

That institutional structure makes it possible to engage external researchers (task 1) and safeguard data (task 2). Even risk-averse scholars engage with confidence on projects that rely on Census Bureau and Bureau of Labor Statistics data at the RDCs because they can plan projects before accessing the data, and once cleared, they know the access will be sustained.[59] Data sent to the RDCs is safeguarded through the combination of controlled systems and vetting.

RDCs or similar structures would not, however, address the full range of issues in task 3. The analytical work is done by scholars with no contractual obligation to the RDCs, so these institutions can only support research of inherent interest to academic researchers. Because there are a wide range of issues that are critical for society and industry, but not necessarily of academic interest, a different solution is required when it comes to political influence operations and other aspects of industry's impact on society.

FFRDCs and UARCs

The history of FFRDCs starkly illustrates how trusted intermediary institutions can meet dynamic and rapidly evolving research needs. FFRDCs "provide federal agencies with R&D capabilities that cannot be effectively met by the federal government or the private sector alone."[60] They are operated on a not-for-profit basis by contractors (including universities and other not-for-profit organizations

such as the RAND Corporation and the MITRE Corporation, which administers FFRDCs), typically through five-year renewable contracts.[61] A given FFRDC is subject to special rules on procurement, contracting, and function, complying with the provisions governing the particular federal agency that sponsors it.[62] In particular, these entities help meet long-term federal research and development requirements with minimal commercial conflicts of interest, while providing a home for highly specialized personnel.[63] Industry actors should draw from the FFRDC experience—in particular the combination of clear sponsor guidelines, strong prohibitions against other commercial work, and time-limited yet flexible contracts—for institutional models that could address key research needs.

The management and governance of FFRDCs is formalized in Section 35.017 of the Federal Acquisition Regulation.[64] Sponsor agencies (such as the Department of Defense) are responsible for oversight of their FFRDCs and must conduct annual audits, performance assessments, and reviews before renewing agreements.[65] Currently, each sponsor agency has its own management processes, and there is no fixed interagency procedure. Annual research plans are created and must be approved by the sponsor agency and the corresponding FFRDC before delegating workloads and assigning hours for tasks.[66]

Similar to FFRDCs, university-affiliated research centers (UARCs) also provide specialized research and expertise to their respective sponsor agencies.[67] While UARCs are not formally defined in federal law, the Department of Defense has codified procedures and rules on their management and operations.[68] UARCs must be university-affiliated and operate out of university or college campuses, have education as a core part of their mission, and remain flexible in terms of competing for public or private contracts.[69] Currently, there are fourteen Department of Defense–operated UARCs.[70]

Both types of institutions can be traced back to World War II, when scientists, engineers, and academics mobilized to support the war effort. Early in the Cold War, such examples of collaboration were formalized in FFRDCs whose mission was to address national security research requirements. The FFRDCs took on niche activities that could not be accomplished directly by the government or by for-profit firms.[71]

The Department of Defense was the first agency to use FFRDCs, as it saw the need for "policy guidance for operations and strategic planning" and "unbiased technical guidance and expertise for major systems developments."[72] As the federal government research agenda has changed over the decades, so has the role and mission of FFRDCs. There have been 123 FFRDCs since 1948, though only forty-two are currently active and sponsored by thirteen federal agencies, according to the National Science Foundation master list.[73]

That flexibility is enabled by rules governing FFRDCs, which provide them with the ability to engage with new challenges as they arise and to shut down when problem sets change.[74] Under the Federal Acquisition Regulation, sponsor agencies are required to reevaluate their FFRDC agreements at least every five years, providing a measure of stability while enabling adaptations to the changing security environment.

FFRDCs address a wide range of issues beyond traditional national security concerns, including terrorist threats, cybersecurity issues, protection of U.S. information technology infrastructure, healthcare, environmental issues, and civil infrastructure modernization.[75] Sometimes these institutions respond to emergency issues. FFRDCs affiliated with the Department of Homeland Security and the Department of Energy, for example, rapidly mobilized technology and explosives experts to assess threats and weaknesses in airport security systems following an attempted airplane bombing on December 25, 2009, and proposed a number of specific improvements.[76] As the misinformation challenge posed by COVID-19, the disease caused by the new coronavirus, has so clearly highlighted, having established institutions capable of expanding research capacity on emergent issues could provide significant value to technology companies. Creating such structures will be key to getting ahead of such problems in the future.

Another key structural element of FFRDCs has been their recruitment of academics through sabbatical periods, consulting arrangements, and competing on the academic job market for core permanent staff. These practices foster the cross-pollination of ideas between government and academia. In RAND's early days, such cross-pollination arguably laid the foundation for the United States' Cold War–era nuclear weapons strategy. The Institute for Defense Analyses (IDA) and other FFRDCs continue these practices to the present day. As with the CFR IAF program, defense-academia connections help the defense community address task 3 beyond the lifetime of any given project.

FFRDC Contracting

The key to how FFRDCs have historically addressed all three key tasks lies in the guidelines of the sponsoring agency agreements. Clear but minimal requirements for these are set out in the admirably terse Federal Acquisition Regulation Section 35.017-1, which outlines the five necessary sections of a sponsoring agency agreement. These nine short sentences have enabled the creation of more than one hundred bespoke research institutions in the last forty years:

1. A statement of the purpose and mission of the FFRDC;
2. Provisions for the orderly termination or nonrenewal of the agreement, disposal of assets, and settlement of liabilities. The responsibility for capitalization of an FFRDC must be defined in such a manner that ownership of assets may be readily and equitably determined upon termination of the FFRDC's relationship with its sponsor(s);

3. A provision for the identification of retained earnings (reserves) and the development of a plan for their use and disposition;
4. A prohibition against the FFRDC competing with any non-FFRDC concern in response to a federal agency request for proposal for other than the operation of an FFRDC. This prohibition is not required to be applied to any parent organization or other subsidiary of the parent organization in its non-FFRDC operations. Requests for information, qualifications, or capabilities can be answered unless otherwise restricted by the sponsor;
5. A delineation of whether or not the FFRDC may accept work from other than the sponsor(s). If non-sponsor work can be accepted, a delineation of the procedures to be followed, along with any limitations as to the non-sponsors from which work can be accepted (other federal agencies, state or local governments, nonprofit or profit organizations, et cetera).[77]

Note how these regulations combine strict prohibitions on competing with commercial firms for federal government work with flexibility of purpose and method. The language does not place strict requirements on what kinds of data the FFRDCs can use, how their studies will be reviewed, what their specific personnel rules should be, or how they should be organized internally. The Federal Acquisition Regulation guidelines effectively allow each FFRDC and its sponsoring agencies to craft an institution that can address their specific problems. Many have built mechanisms for prioritizing research in collaboration with the sponsoring agency while also allowing entrepreneurial activity by researchers at the FFRDC. Those researchers can work collaboratively with potential government sponsors to define projects and execute them, effectively enabling personnel at supported agencies to flexibly access the research capacity at the FFRDCs.[78]

The Department of Defense, for example, incorporates guidelines for work performance within its sponsor agreements with FFRDCs. Broadly, proposed projects go through several stages to determine whether they are appropriate and align with a given FFRDC's core competencies.[79]

Of course, the FFRDC structure is no panacea. They have historically faced challenges and criticism from their customers, Congress, and academia. Challenges include the need to prioritize and defer projects due to congressionally imposed limits on annual working hours and staffing levels, as well as infrastructure modernization issues and concerns over competition with other military-funded projects.[80] Historically, RAND and other FFRDCs faced criticism for their involvement in the Vietnam War, consistent with widespread, anti-war sentiment at universities and among the general public.[81] The study that aroused the most public ire showed that U.S. forces were succeeding in demoralizing enemy forces through repeated attacks, including large-scale, aerial bombardment.[82] That study was allegedly used to justify continuing combat operations, leading to protests against university associations with the military at many campuses. Some of those incidents escalated to physical assaults on facilities, including at least one bombing with casualties.[83]

Interestingly, that study was just one of a series seeking to better understand enemy motivation and morale. At least one of the studies in the series yielded opposing findings, suggesting that U.S. combat operations were ineffective in reducing enemy motivation and morale.[84] That study's publication and the controversy it caused within the government actually highlight the important role FFRDCs have played in bringing forward evidence that contradicts the preferences of senior policymakers.

Overall, the FFRDC's contract arrangements have enabled research on sensitive topics with secret data while still allowing for an important measure of independence and publication of heterodox findings. That combination could be helpful for making progress on the broad issue of influence operations where the core data involve significant privacy concerns, the companies holding it need some control over research, yet society as a whole could benefit from findings that are uncomfortable for the platforms.

IDA and Lessons for Cross-Platform Data Sharing

The IDA merits special mention because of its ability to work with government and private sector partners on projects involving proprietary commercial data without the protections of the national security classification system. The origins of the IDA lie with the Weapons System Evaluation Group (WSEG). The WSEG was established in December 1948 as a high-level advisory group to serve the Joint Chiefs of Staff and the Secretary of Defense.[85] It was intended to combine military and civilian expertise to achieve three primary objectives: to bring scientific, technical, and operational military expertise to bear in evaluating weapons systems; to employ advanced techniques of scientific analysis and research; and to approach its tasks from an impartial perspective that transcended the various branches of the armed forces.

Eventually, as demands on WSEG continued to strain its small staff and limited resources, Department of Defense authorities considering the contractual alternatives available for WSEG realized university sponsorship could lend greater scientific prestige to the enterprise while attracting more civilian research analysts and enabling closer ties to the academic community.[86] Toward this end, the Secretary of Defense and Joint Chiefs of Staff convened a group of leading universities to sponsor a nonprofit corporation to assist WSEG in addressing some of the country's most pressing security issues. The organization, formally incorporated as the IDA, was established in 1956 by five university members.[87] Cooperation between academia and government was key to establishing the new institution.

The IDA has dealt with proprietary information from multiple companies competing for multimillion and sometimes multibillion-dollar contracts. That it can do so across multiple competing firms (for example, Lockheed Martin or Boeing) on multibillion-dollar procurement contracts is a testament to the power of its institutional model and the strict noncompete provisions discussed above. Personnel who work on technology assessments get to know their industry counterparts very well and have authority to see full cost structures. Yet the IDA remained a trusted interlocutor for cost-effectiveness analysis. Firms are comfortable sharing proprietary information with the IDA because they knew the organization has strong security protections in place and that its contracts prevented it from monetizing any information it receives. All the incentives are aligned for protecting proprietary information. Critically, much of this information sharing happens without the legal protections of the national security classification system. It is enabled by the combination of clear contractual incentives and a long-run culture of treating proprietary data with great care.

Benefits of Intermediate Organizations

Lessons learned from the FFRDC experience can inform society's widely shared objective of addressing influence operations on social media platforms. Democratic governments around the world are interested in better understanding the nature of influence operations to protect their societies and defend the integrity of their elections. Similarly, technology companies want to address this phenomenon because they face reputational and business risks for failing to mitigate malign influence operations.

A key challenge in addressing influence operations is building the stable, objective, independent R&D capacity necessary to tackle the problem. The long-running relationship between researchers and the U.S. federal government provides many lessons for how to do this. While formal institutions for government-academia data sharing have played a role, and while informal relationships have enabled a large body of excellent work over the years—some of which guided strategy for how to avoid the literal end of the world through nuclear conflict at the height of the Cold War—organizations that sat between the government and academia also played a central role.

How FFRDCs Fit In

The structure of FFRDCs—the long-term commitment to the sponsor, a lack of commercial conflicts of interest, and the retention of high-skilled expertise—allows them to address all three critical tasks for tech-academia collaboration. They routinely work with classified and proprietary data (task

1). Their reputations and internal peer-review processes provide credibility even when full soup-to-nuts replication data cannot be made public in the tradition of open science (task 2).[88] And, importantly, the close relationship between FFRDCs and their sponsoring agencies has not prevented them from publishing heterodox findings (task 3).

Over the years FFRDCs have done research on a wide range of sensitive topics. Recently these include the inherent challenges of assessing progress in counterinsurgency campaigns (citing mistakes made by U.S. forces in Afghanistan and Iraq) and the many failures of the federal government's so-called war on drugs.[89] Similarly, JASON, a program run out of MITRE though not technically an FFRDC, provided a highly controversial outside assessment of the Department of Energy's Lifetime Extension Program for deployed nuclear weapons in 2009.[90]

When it comes to maintaining credibility and engaging external researchers (task 1)—FFRDCs and related organizations have long provided a venue for developing skilled researchers and connections. And they have worked out standards regarding research integrity that create credibility. For example, a measure of independence from government manipulation of studies is baked into sponsoring agency agreements and internal standards, which typically specify mechanisms for peer-review and limit the government's ability to restrict publication. Such rules create contractual protections for researcher independence. While tacit government influence over FFRDC work is always present because researchers at FFRDCs have long-term relationships to maintain with officials at their sponsoring agencies, contractual independence has enabled these institutions to tackle a wide range of sensitive topics and regularly publish controversial findings.

As for safeguarding data while enabling cross-platform research (task 2)—IDA's success in managing data security and trust issues between multiple industry actors stands out. It demonstrates that properly structured contracts combined with institutional prohibitions on other kinds of for-profit work can address many concerns, even without the protections of the national security classification system.

Finally, the codified research initiation mechanisms at various FFRDCs often helped with overcoming institutional barriers (task 3) by allowing mid-level personnel in government to get work done without getting senior leaders' approval, exempting them from the usually lengthy processes related to drafting proposals, getting authorization, and securing funding. Ironically, having structured processes for setting the research agenda ultimately enabled a nimble and dynamic research approach that cut through the bureaucratic obstacles typical of secure government initiatives. The entire procedure—from identifying an area of concern for R&D efforts to ultimately dispersing funds—was greatly simplified.

Certain FFRDC models also incorporated an element of competition to ensure efficiency. In the Department of Defense approach, for example, offices could invite multiple FFRDCs to bid on the opportunity to pursue a given research objective. Allowing the requesting office to compare the capabilities of each and identify the best-equipped organization for the job served to keep quality up and costs down without the full set of lengthy contracting procedures required for open procurement.

Overall, FFRDCs and related institutions allowed the government to benefit from the contributions of top scientific talent. Early on, many were drawn by the organizations' prestige. To this day, FFRDCs routinely attract scientists who do not want to work directly for the government, at least not for their entire careers.

Making the FFRDC model work required support in terms of federal government contracting rules, willing sponsors, and, most importantly, a strong demand for research over decades. There are more than seventy years of history behind the FFRDC ecosystem. The growth of these entities in the early post–World War II period was driven by the conviction that the government needed help from people who would not work for it directly but would work for one of these institutions. That growth was enabled by contracting rules in two respects. First, the rules prohibited FFRDCs from competing on for-profit contracts, which meant they posed no threat to companies in terms of their material interests. Second, the government retained ultimate release control for the most sensitive studies, limiting reputational and security risks.

To be sure, the FFRDC model and other intermediate solutions fall well short of the open-science ideal. They do not expand the set of researchers in a democratic manner (in the sense of allowing a diverse set of scholars to self-select into working with data). And peer-review for classified work has to happen in a constrained manner, primarily by others inside the intermediate institutions. But it is exactly because they compromise on some of the open-science ideals that they can overcome the kind of data-sharing constraints that currently stymie a wide range of potentially beneficial work.

From Tasks to Principles

This study began by identifying three key unmet tasks: maintaining credibility and engaging external researchers, safeguarding data while enabling cross-platform research, and overcoming structural barriers. In the defense community, a range of institutions have solved some or all of these issues. In particular, the basic principles laid out in the Federal Acquisition Regulation for FFRDCs have supported a rich ecosystem of organizations that have addressed a huge variety of scientific problems over seven decades.

Industry leaders and academics interested in countering influence operations should draw inspiration from that history and begin thinking about the principles that would allow a similar sort of ecosystem to flourish and address their problems. Such principles could also be useful in building organizations to tackle the wider set of practical research and development challenges around social media's impact on society.

So what principles should guide the development of intermediate organizations that would bring similar capabilities to the challenge of countering malicious influence operations as FFRDCs brought to the defense community? Five stand out: longevity, collaborative prioritization, professional staff, noncompete provisions, and peer review.

1. **Longevity:** Any new intermediate organization must have sustained funding for a number of years that is not subject to changes in sponsor priorities. This could be accomplished, for example, through the creation of a trust by several social media firms.
2. **Collaborative prioritization:** Each organization should have a sponsoring agreement by which firms would articulate what topics they would want a new organization to work on and establish an annual process for allocating that organization's resources.
3. **Professional staff:** Core personnel should be drawn from a combination of research and tech communities, along the lines of the LAS model, with senior staff hired on multiyear contracts to provide the stability top-notch researchers will demand.
4. **No competition:** Organizations should be nonprofits or B-corporations in structure, the by-laws of which enshrine strong privacy protections and restrict them from bidding on work for companies they are sharing data with or those firms' competitors.
5. **Peer review:** The ability to withstand the criticism of other scholars is the cornerstone of scientific credibility. These organizations need a set of standards for peer review, as well as prepublication advisory review and comment by the technology companies. The latter will ensure companies have a chance to provide feedback and reduce their concerns about erroneous findings. In this setting, peer review could be modeled on the Government Accountability Office's protocols, which mandate that the organization solicit agency comments before publication and include response to those comments in its reports.[91] Properly institutionalizing research independence would go a long way toward enhancing the credibility of new organizations while also addressing recruiting challenges.

Work could begin today on model contracts and agreements to instantiate those principles. Having them would make it much easier for industry to support institutions that can carry out the vast volume of critical research that sits in the gray world between what companies can do themselves and what could be done by academics given data-sharing constraints.

If the long experience of developing the FFRDC and UARC ecosystem is any guide, one single brilliant model solving all problems inhibiting tech-academia collaboration on influence operations is unlikely. Instead, there will be a process of innovation in which the right set of principles enables many different solutions to be tried. Some will fail, but others will succeed and help address the problems posed by malign information operations. That kind of entrepreneurial process is one technology companies should be able to get behind.

Conclusion

While industry actors are making substantial efforts to address complex challenges like those posed by online influence operations, more must be done with an eye toward the future. Social media companies face obstacles to user trust and safety that will endure and likely intensify over time. This is perhaps more evident at the time of this writing than ever before, as misinformation surrounding the coronavirus pandemic continues to spread, threatening public health in countries around the world.

Nongovernmental organizations and academic institutions have responded quickly to some aspects of what United Nations officials have termed an "infodemic."[92] Fact-checking organizations in dozens of countries soon began debunking false claims, and a number of organizations, including ESOC, began collecting data on disinformation narratives.[93] The major social media platforms took action to remove known misinformation, albeit with varying levels of success, sometimes spurred on by research showing their efforts were not yet highly effective.[94] And researchers moved quickly to understand who was spreading coronavirus-related misinformation on some platforms. Encouraging as these ad hoc efforts may be, they surely fell short of what could have been done had there been established research institutions that could turn to the problem with deep data access, technical capacity, and personnel skilled in working with social media data.

Efforts to build institutions equipped with the needed research capacity and cross-disciplinary expertise to tackle misinformation across platforms could draw heavily on lessons from the long history of defense-academia collaborations. The diverse organizational ecosystem around defense-relevant R&D demonstrates that there are ways to meet the three critical tasks of this endeavor. Establishing knowledge-sharing institutions will be critical to addressing current problems facing technology companies—such as nation-state-led information operations and the increasing use of synthetic videos—and will build readiness to get ahead of future crises.

About the Authors

Jacob N. Shapiro is a professor of politics and international affairs at Princeton University whose research covers conflict, economic development, and security policy.

Contact: Department of Politics and Woodrow Wilson School of Public and International Affairs, Princeton University, Princeton, NJ 08540. Email: jns@princeton.edu

Michelle P. Nedashkovskaya is a Master of Public Affairs candidate at the Woodrow Wilson School of Public and International Affairs at Princeton University and a research assistant with the Empirical Studies of Conflict Project.

Contact: Woodrow Wilson School of Public and International Affairs, Princeton University, Princeton, NJ 08540. Email: mpn@princeton.edu

Jan G. Oledan is a research specialist with the Empirical Studies of Conflict Project at Princeton University.

Contact: Empirical Studies of Conflict Project, Princeton University, Princeton, NJ 08540. Email: joledan@princeton.edu

Acknowledgments

The authors thank Vlad Barash, Steve Biddle, David Broniatowski, David Chu, Steve Downs, Joe Felter, Michael C. Horowitz, Radha Iyengar, Seth Jones, Damon McCoy, Ben Nimmo, Nate Persily, Scott Sagan, Caitlin Talmadge, Josh Tucker, Alicia Wanless, Chris White, and Alyson Wilson for helpful suggestions, deep thoughts, and direction to relevant citations. The paper benefited tremendously from feedback at the meeting on enabling industry-academic collaboration hosted by the Carnegie Endowment for International Peace.

This research was supported in part by a gift from Microsoft. Shapiro has previously served on paid advisory groups for Facebook and Twitter and has been an adjunct at the RAND Corporation. All errors are the responsibility of the authors.

Notes

1 Panayiota Tstatsou, "Social Media and Informal Organisation of Citizen Activism: Lessons From the Use of Facebook in the Sunflower Movement," *Social Media + Society* 4, no. 1 (January–March 2018): 1-12, https://doi.org/10.1177%2F2056305117751384.

2 Diego Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent Trends in Online Foreign Influence Efforts," *Journal of Information Warfare* 18, no. 3 (2019): 15–48, https://www.jinfowar.com/journal/volume-18-issue-3/recent-trends-online-foreign-influence-efforts; and Fergus Hanson, Sarah O'Connor, Mali Walker, and Luke Courtois, "Hacking Democracies," Australian Strategic Policy Institute, May 15, 2019, http://www.aspi.org.au/report/hacking-democracies.

3 David Klepper and Danica Kirka, "Tech Companies Rush to Fight Misinformation Ahead of UK Vote," Associated Press, November 10, 2019, https://apnews.com/1e2a9c09f6774fdea811dafe2b2cdf45.

4 As Joshua Tucker and Nathaniel Persily point out, there is a tremendous volume of research that leverages social media data to answer obviously product-relevant question being done by platforms and their partners. See Nathaniel Persily and Joshua A. Tucker, "The Challenges and Opportunities for Social Media Research," in *Social Media and Democracy: The State of the Field,* edited by Nathaniel Persily and Joshua A. Tucker (Cambridge: Cambridge University Press), 2020.

5 Claes de Vreese, Marco Bastos, Frank Esser, Fabio Giglietto, Sophie Lecleher, Barbara Pfetsch, Cornelius Puschmann, Rebekah Tromble, Gary King, and Nathaniel Persily, "Public Statement From the Co-Chairs and European Advisory Committee of Social Science One," Social Science One, December 11, 2019, https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one.

6 Andy Greenberg, "Facebook's Ex-Security Chief Details His 'Observatory' for Internet Abuse," *Wired*, July 25, 2019, https://www.wired.com/story/alex-stamos-internet-observatory/.

7 See, for example, Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson, "Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse," presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13) (2013), 195–210; Kurt Thomas, Dmytro Iatskiv, Elie Bursztein, Tadek Pietraszek, Chris Grier, and Damon McCoy, "Dialing Back Abuse on Phone Verified Accounts," 2014 ACM SIGSAC Conference on Computer and Communications Security, 465–476; Kurt Thomas, Juan A. Elices Crespo, Ryan Rasti, Jean-Michel Picod, Cait Phillips, Marc-André Decoste, Chris Sharp et al., "Investigating Commercial Pay-per-Install and the Distribution of Unwanted Software," 25th {USENIX} Security Symposium ({USENIX} Security 16) 2016, 721–739; and Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy, "Evaluating Login Challenges as a Defense Against Account Takeover," The World Wide Web Conference (2019), 372–382.

8 Short-term means the next quarter or next year. By comparison, most social science research projects take multiple years from conceptualization to publication.

9 Gary King and Nathaniel Persily, "A New Model for Industry-Academic Partnerships," *PS: Political Science & Politics* (2019): 1–7, https://doi.org/10.1017/S1049096519001021.

10 Nathaniel Gleicher, "How We Respond to Inauthentic Behavior on Our Platforms: Policy Update," Facebook Newsroom, October 21, 2019, https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/.

11 Recent work from the Stanford Internet Observatory suggests that Google has been relatively effective at removing fake news from its search results compared to Bing. See Daniel Bush and Alex Zaheer, "Bing's Top Search Results Contain an Alarming Amount of Disinformation," Stanford Internet Observatory, December 17, 2019, https://cyber.fsi.stanford.edu/io/news/bing-search-disinformation; "How Google Fights Disinformation," Google, February 2019, https://www.blog.google/documents/37/HowGoogleFightsDisinformation.pdf.

12 Peter Talbot, "Twitter Removes Thousands of Accounts for Manipulating Its Platform," NPR, September 20, 2019, https://www.npr.org/2019/09/20/762799187/twitter-removes-thousands-of-accounts-for-manipulating-their-platform; and Sara Harrison, "Twitter's Disinformation Dumps Are Helpful—to a Point," *Wired*, July 7, 2019, https://www.wired.com/story/twitters-disinformation-data-dumps-helpful/.

13 The major platforms have all released documents detailing relevant policy updates and efforts to reduce inauthentic behavior across their products. See Kristie Canegallo, "Fighting Disinformation Across Our Products," Keyword, February 16, 2019, https://www.blog.google/around-the-globe/google-europe/fighting-disinformation-across-our-products/; Colin Crowell, "Our Approach to Bots and Misinformation," Twitter Blog, June 14, 2017, https://blog.twitter.com/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html; and Monika Bickert, "Enforcing Against Manipulated Media," Facebook Newsroom, January 6, 2020, https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/.

14 Sebastian Bay and Rolf Fredheim, "How Social Media Companies Are Failing to Combat Inauthentic Behaviour Online," NATO Strategic Communications Center of Excellence, November 2019, https://www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online.

15 Carroll Doherty and Jocelyn Kiley, "Americans Have Become Much Less Positive About Tech Companies' Impact on the U.S.," Pew Research Center, July 29, 2019, https://www.pewresearch.org/fact-tank/2019/07/29/americans-have-become-much-less-positive-about-tech-companies-impact-on-the-u-s/.

16 Herb Weisbaum, "Trust in Facebook Has Dropped by 66 Percent Since the Cambridge Analytica Scandal," NBC News, April 18, 2018, https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011.

17 Louise Matsakis, "Why Facebook's Banned 'Research' App Was So Invasive," *Wired*, January 30, 2019, https://www.wired.com/story/facebook-research-app-root-certificate/

18 Charles Arthur, "Facebook Emotion Study Breached Ethical Guidelines, Researchers Say," *Guardian*, June 30, 2014, https://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say; and Kaitlyn Tiffany, "Facebook Has Been Paying Minors $20 for Access to All of Their Personal Data," *Vox*, January 30, 2019, https://www.vox.com/the-goods/2019/1/30/18203803/facebook-research-vpn-minors-data-access-apple.

19 Lily Hay Newman, "No One Can Get Cybersecurity Disclosure Just Right—Especially Lawmakers," *Wired*, October 12, 2018, https://www.wired.com/story/cybersecurity-disclosure-gdpr-facebook-google/.

20 Annie Franco, Neil Malhotra, and Gabor Simonovits, "Publication Bias in the Social Sciences: Unlocking the File Drawer," *Science* 345, no. 6203 (September 2014): 1502–1505, https://science.sciencemag.org/content/345/6203/1502/tab-pdf.

21 Though, as discussed in the second part of this paper, some defense research organizations have managed to work with highly valuable proprietary data from multiple firms quite well over the years.

22 In 2017, the average employee turnover rate in the tech sector was 13.2 percent—the highest of any industry. See Michael Booz, "These 3 Industries Have the Highest Talent Turnover Rates," LinkedIn Talent Blog, March 15, 2018, https://business.linkedin.com/talent-solutions/blog/trends-and-research/2018/the-3-industries-with-the-highest-turnover-rates.

23 David J. Teece, "Firm Organization, Industrial Structure, and Technological Innovation," *Journal of Economic Behavior Organization* 31, no. 2 (November 1996): 193–224, http://www.sciencedirect.com/science/article/pii/S0167268196008955; and Grant Freeland, "Oh No, Not Another Reorganization! Do We Really Need One?" *Forbes*, November 5, 2018, https://www.forbes.com/sites/grantfreeland/2018/11/05/oh-no-not-another-reorganization-do-we-really-need-one/.

24 Jacob Metcalf, Emanuel Moss, and Danah Boyd, "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics," *Social Research: An International Quarterly* 86, no. 2 (Summer 2019): 449–476, https://muse.jhu.edu/article/732185.

25 This study examined the organizational approaches of six other institutions for this work: Digital Intelligence Lab, see "Digital Intelligence Lab," Institute for the Future, http://www.iftf.org/partner-with-iftf/research-labs/digital-intelligence-lab/; Digital Forensic Research Lab (DFRL), see: "Digital Forensics Research Lab," Atlantic Council, https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/; Hamilton 2.0 Dashboard, see: "Hamilton 2.0 Dashboard," German Marshall Fund Alliance for Securing Democracy, https://securingdemocracy.gmfus.org/hamilton-dashboard/; Computational Propaganda Project, see: "About," The Computational Propaganda Project at the University of Oxford's Oxford Internet Institute, https://comprop.oii.ox.ac.uk/about-the-project/; Cyber Policy Center, see: "International Cyber Policy Center," Australian Strategic Policy Institute, https://www.aspi.org.au/program/international-cyber-policy-centre; and East StratCom Task Force, see "Questions and Answers About the East StratCom Task Force," European Union External Action Service, December 5, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en. DFRL's long-running collaboration with Facebook is the clearest example of a successful multiyear partnership between an external research organization and a social media platform, but the partnership's remit so far appears limited to descriptive work on political influence campaigns. See Issie Lapowsky, "Inside the Research Lab Teaching Facebook About Its Trolls," *Wired*, August 15, 2018, https://www.wired.com/story/facebook-enlists-dfrlab-track-trolls/; and Graham Brookie, "Why We're Partnering With Facebook on Election Integrity," Medium, May 17, 2018, https://medium.com/dfrlab/why-were-partnering-with-facebook-on-election-integrity-19f0ca39db2e.

26 "Overview," Social Science One, https://socialscience.one/overview.

27 Jeffrey Mervis, "Privacy Concerns Could Derail Unprecedented Plan to Use Facebook Data to Study Elections," *Science*, September 24, 2019, https://www.sciencemag.org/news/2019/09/privacy-concerns-could-derail-unprecedented-plan-use-facebook-data-study-elections.

28 Alex Pasternack, "Frustrated Funders Exit Facebook's Election Transparency Project," Fast Company, October 28, 2019, https://www.fastcompany.com/90412518/facebooks-plan-for-radical-transparency-was-too-radical; and Daniel Stid, "Taking Stock of an Initial Project to Understand Social Media's Impact on Democracy," William and Flora Hewlett Foundation, February 13, 2020, https://hewlett.org/taking-stock-of-an-initial-project-to-understand-social-medias-impact-on-democracy/.

29 The authors thank Alicia Wanless for reminders of these issues. See also Craig Scribner, "Data Disorganization Is a Big Problem," Claravine, May 7, 2019, https://www.claravine.com/2019/05/07/data-disorganization-is-a-big-problem/; and Richard Carufel, "Data Overload Isn't Just About Volume—It's Also About Disorganization," Agility PR Solutions, November 13, 2017, https://www.agilitypr.com/pr-news/public-relations/data-overload-isnt-just-volume-also-disorganization/.

30 Thomas C. Schelling, *Strategy of Conflict* (Cambridge: Harvard University Press, 1980); and Albert Wohlstetter, "The Delicate Balance of Terror," RAND Corporation, 1958, https://www.rand.org/pubs/papers/P1472.html.

31 Scott Douglas Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1993).

32 Michael C. Horowitz, "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence, and Stability," *Journal of Strategic Studies* 42, no. 6 (2019): 764–788, https://doi.org/10.1080/01402390.2019.1621174; Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "Separating Fact From Fiction in the Debate Over Drone Proliferation," *International Security* 41, no. 2 (Fall 2016): 7–42, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00257; and Matthew Fuhrmann and Michael C. Horowitz, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles," *International Organization* 71, no. 2 (Spring 2017): 397–418, https://doi.org/10.1017/S0020818317000121.

33 Charles D. Allen and Edward J. Filiberti, "The Future of Senior Service College Education: Heed the Clarion Call," *Joint Forces Quarterly* 81, no. 2 (April 2016): 51, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-81/Article/702020/the-future-of-senior-service-college-education-heed-the-clarion-call/.

34 For more, see "About Us," Empirical Studies of Conflict, https://esoc.princeton.edu/about-us.

35 ESOC's other director, retired colonel Joseph Felter, was an active duty Army officer when the project started, resigned his role at ESOC to serve as the deputy assistant secretary of defense for South Asia and has now resumed his role with ESOC in addition to his position as a research fellow at the Hoover Institution.

36 Luke N. Condra, James D. Long, Andrew C. Shaver, and Austin L. Wright, "The Logic of Insurgent Electoral Violence," *American Economic Review* 108, no. 11 (November 2018): 3199–3231, https://www.aeaweb.org/articles?id=10.1257/aer.20170416; Eli Berman, Jacob N. Shapiro, and Joseph H. Felter, "Can Hearts and Minds Be Bought? The Economics of Counterinsurgency in Iraq," *Journal of Political Economy,* 119, no. 4 (August 2011): 766–819, https://www.jstor.org/stable/10.1086/661983?seq=1; Gabriela Calderón, Gustavo Robles, Alberto Díaz-Cayeros, and Beatriz Magaloni, "The Beheading of Criminal Organizations and the Dynamics of Violence in Mexico," *Journal of Conflict Resolution* 59, no. 8 (December 2015): 1455–1485, https://doi.org/10.1177/0022002715587053; and Benjamin Crost, Joseph Felter, and Patrick Johnston, "Aid Under Fire: Development Projects and Civil Conflict," *American Economic Review* 104, no. 6 (June 2014): 1833–1856, https://www.aeaweb.org/articles?id=10.1257/aer.104.6.1833.

37 Joseph Felter, Jeff Bramlett, Bill Perkins, Jarret Brachman, Brian Fishman, James Forest, Lianne Kennedy, Jacob Shapiro, and Tom Stocking, "Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities," Combatting Terrorism Center at West Point, February 14, 2006, https://www.ctc.usma.edu/harmony-and-disharmony-exploiting-al-qaidas-organizational-vulnerabilities/; Jacob N. Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations* (Princeton: Princeton University Press, 2013); Benjamin W. Bahney, Radha K. Iyengar, Patrick B. Johnston, Danielle F. Jung, Jacob N. Shapiro, and Howard J. Shatz, "Insurgent Compensation: Evidence from Iraq," *American Economic Review: Papers and Proceedings* 103, no. 3 (May 2013): 518–522, https://www.aeaweb.org/articles?id=10.1257/aer.103.3.518; and Patrick B. Johnston, Jacob N. Shapiro, Howard J. Shatz, Benjamin Bahney, Danielle F. Jung, Patrick Ryan, and Jonathan Wallace, *Foundations of the Islamic State: Management, Money, and Terror in Iraq, 2005–2010* (Santa Monica: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1192.html.

38 Stephen Biddle, Jeffrey A. Friedman, and Jacob N. Shapiro, "Testing the Surge: Why Did Violence Decline in Iraq in 2007?," *International Security* 37, no. 1 (Summer 2011): 7–40, https://www.jstor.org/stable/23280403; and Jacob N. Shapiro and Nils B. Weidmann, "Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq," *International Organization* 69, no. 2 (Spring 2015): 247–274, https://doi.org/10.1017/S0020818314000423.

39 Jonathan Lehne, Jacob N. Shapiro, and Oliver Vanden Eynde, "Building Connections: Political Corruption and Road Construction in India," *Journal of Development Economics* 131 (March 2018):62–78, https://doi.org/10.1016/j.jdeveco.2017.10.009.

40 The time horizon for improving informal engagements is much shorter than for creating new organizations or enacting regulatory changes to facilitate research cooperation. In these authors' recent experience working with technology companies on countering disinformation campaigns, they found that relationship building can help overcome the combination of legal and public relations issues that creates barriers at the edges of companies.

41 This is also true for the LAS model discussed later in the paper.

42 The authors thank Radha Iyengar for suggesting this particular framing.

43 Alyson Wilson, Matthew Schmidt, Lara Schmidt, and Brent Winter, "Immersive Collaboration on Data Science for Intelligence Analysis," *Harvard Data Science Review* 1, no. 2 (November 2019), https://doi.org/10.1162/99608f92.4a9eef8d; see also "Laboratory for Analytic Sciences," North Carolina State University, https://ncsu-las.org/.

44 Kathleen M. Vogel, Jessica Katz Jameson, Beverly B. Tyler, Sharon Joines, Brian M. Evans, and Hector Rendon, "The Importance of Organizational Innovation and Adaptation in Building Academic–Industry–Intelligence Collaboration: Observations From the Laboratory for Analytic Sciences," *International Journal of Intelligence, Security, and Public Affairs* 19, no. 3 (2017): 173, https://doi.org/10.1080/23800992.2017.1384676.

45 Kathleen M. Vogel and Beverly B. Tyler, "Interdisciplinary, Cross-sector Collaboration in the U.S. Intelligence Community: Lessons Learned From Past and Present Efforts," *Intelligence and National Security* 34, no. 6 (June 2019): 851–880, https://doi.org/10.1080/02684527.2019.1620545.

46 Vogel et al., "The Importance of Organizational Innovation and Adaptation in Building Academic–Industry–Intelligence Collaboration"; and Wilson et al., "Immersive Collaboration on Data Science for Intelligence Analysis."

47 "A Selected History of DARPA Innovation," Defense Advanced Research Projects Agency, https://www.darpa.mil/Timeline/index.html; and Marcy E. Gallo, "Defense Advanced Research Projects Agency: Overview and Issues for Congress," Congressional Research Service, updated March 17, 2020, https://fas.org/sgp/crs/natsec/R45088.pdf.

48 Regina E. Dugan and Kaigham J. Gabriel, "'Special Forces' Innovation: How DARPA Attacks Problems," *Harvard Business Review* 91, no.10 (October 2013): 74–84, https://hbr.org/2013/10/special-forces-innovation-how-darpa-attacks-problems.

49 Jeffrey Mervis, "What Makes DARPA Tick?" *Science* 351, no. 6273 (February 2016): 549–553, https://science.sciencemag.org/content/351/6273/549.summary.

50 Gallo, "Defense Advanced Research Projects Agency," 5.

51 "Innovation at DARPA," Defense Advanced Research Projects Agency, July 2016, https://www.darpa.mil/attachments/DARPA_Innovation_2016.pdf, 3.

52 Gallo, "Defense Advanced Research Projects Agency," 5.

53 Erica R.H. Fuchs, "Cloning DARPA Successfully," *Issues in Science and Technology* 26, no. 1 (Fall 2009): 67, https://www.jstor.org/stable/43315003?seq=1.

54 Gallo, "Defense Advanced Research Projects Agency," 6.

55 Other institutions such as the Department of Energy's eighteen National Laboratories also bring academic talent to bear on sensitive technology issues. Their institutional model is optimized for "large scale, complex research and development challenges" such as fusion energy or the safety and reliability of the United States' nuclear weapons. See "About," Princeton Plasma Physics Laboratory, https://www.pppl.gov/about; and "About," Lawrence Livermore National Laboratory," https://www.llnl.gov/about.

56 "Federal Statistical Research Data Centers," United States Census Bureau, https://www.census.gov/fsrdc.
57 "Secure Research Environment," United States Census Bureau, https://www.census.gov/about/adrm/fsrdc/about/secure_rdc.html.
58 Jung Ho Choi and Brandon Gipper, "Fraudulent Financial Reporting and the Consequences for Employees," Center for Economic Studies Working Paper 19-12, U.S. Census Bureau, March 2019, https://ideas.repec.org/p/cen/wpaper/19-12.html; David J. Brown, Misty L. Heggeness, Suzanne M. Dorinski, Lawrence Warren, and Moises Yi, "Predicting the Effect of Adding a Citizenship Question to the 2020 Census," Center for Economic Studies Working Paper 19-18, U.S. Census Bureau, June 2019, https://ideas.repec.org/p/cen/wpaper/19-18.html; and Danielle Sandler and Nichole Szembrot, "Maternal Labor Dynamics: Participation, Earnings, and Employer Changes," Center for Economic Studies Working Paper 19-33, U.S. Census Bureau, December 2019, https://ideas.repec.org/p/cen/wpaper/19-33.html.
59 In comparison, starting projects requiring data sharing from technology companies is very high risk.
60 Marcy E. Gallo, "Federally Funded Research and Development Centers (FFRDCs): Background and Issues for Congress," Congressional Research Service, December 1, 2017, https://fas.org/sgp/crs/misc/R44629.pdf.
61 Government Accountability Office, "Opportunities Exist to Improve the Management and Oversight of Federally Funded Research and Development Centers," Government Accountability Office Report to Congressional Committees, Publication No. 09-15, October 2008, https://www.gao.gov/assets/290/282697.pdf; Defense Business Board, "Future Models for Federally Funded Research and Development Center Contracts," Report to the Secretary of Defense, 2016, https://dbb.defense.gov/Portals/35/Documents/Reports/2017/DBB%20FY17-02%20FFRDCs%20Completed%20Study%20(October%202016).pdf.
62 Gallo, "Federally Funded Research and Development Centers"; Office of Technology Assessment, *A History of the Department of Defense Federally Funded Research and Development Centers* (Washington, DC: U.S. Government Printing Office, 1995), https://www.princeton.edu/~ota/disk1/1995/9501/9501.PDF.
63 Government Accountability Office, "DOD's Use of Study and Analysis Centers," Government Accountability Office Report to Congressional Committees, Publication No. 20–31, December 2019, https://www.gao.gov/assets/710/703063.pdf.
64 "Federal Acquisition Regulation," *Code of Federal Regulations*, title 48 (2007), § 35.017. Accessible at https://www.acquisition.gov/browse/index/far.
65 Government Accountability Office, "Opportunities Exist to Improve the Management and Oversight of Federally Funded Research and Development Centers," 15.
66 Ibid.
67 Hruby et al., "The Evolution of Federally Funded Research and Development Centers," 20.
68 Department of Defense, "University Affiliated Research Center (UARC) Management Plan," U.S. Department of Defense, July 2010, https://rt.cto.mil/wp-content/uploads/2019/09/UARC-Mgmt-Plan-Jun-23-10-FINAL-6811-with-Signed-Memo.pdf.
69 Hruby et al., "The Evolution of Federally Funded Research and Development Centers," 20.
70 "Federally Funded Research and Development Centers and University Affiliated Research Centers," Defense Innovation Marketplace, https://defenseinnovationmarketplace.dtic.mil/ffrdcs-uarcs/.
71 Government Accountability Office, "DOD's Use of Study and Analysis Centers," Government Accountability Office Report to Congressional Committees, Publication No. 20-31, December 2019, https://www.gao.gov/assets/710/703063.pdf.

72 Bruce C. Dale and Timothy D. Moy, "The Rise of Federally Funded Research and Development Centers," Sandia National Laboratories, September 2000, 9, https://www.semanticscholar.org/paper/The-Rise-of-Federally-Funded-Research-and-Centers-Dale-Moy/0a3e4f324db8d8951b6ec29d5d4e69060ef41f00.

73 The Department of Energy and Department of Defense sponsor the highest numbers of FFRDCs at sixteen and ten respectively. See "Master Government List of Federally Funded R&D Centers," National Science Foundation, https://www.nsf.gov/statistics/ffrdclist/#agency.

74 More than sixty Department of Defense FFRDCs have ceased operations—though some have continued operating in other forms. See Office of Technology Assessment, *A History of the Department of Defense Federally Funded Research and Development Centers*, 6.

75 MITRE, "FFRDCs—A Primer."

76 Jill M. Hruby, Dawn K. Manley, Ronald E. Stoltz, Erik K. Webb, and Joan B. Woodard, "The Evolution of Federally Funded Research and Development Centers," *Public Interest Report* 64, no. 1 (Spring 2011): 29, https://fas.org/pubs/pir/2011spring/FFRDCs.pdf.

77 "Federal Acquisition Regulation," *Code of Federal Regulations*, title 48 (2007), § 35.017, https://www.acquisition.gov/browse/index/far.

78 For example, Shapiro's co-authors Patrick Johnston and Howard Shatz, both social scientists at RAND, found government sponsors to support their work on the research that led to *Foundations of the Islamic State: Management, Money, and Terror in Iraq, 2005–2010*.

79 The Government Accountability Office summarizes processes for project initiation at different FFRDCs under various sponsors. See Government Accountability Office, "Opportunities Exist to Improve the Management and Oversight of Federally Funded Research and Development Centers," 16-18.

80 Government Accountability Office, "DOD's Use of Study and Analysis Centers," 10; and Government Accountability Office, "Defense Science and Technology: Actions Needed to Enhance Use of Laboratory Initiated Research Authority," Government Accountability Office Report to Congressional Committees, Publication No. 19-64, December 2018, 35, https://www.gao.gov/assets/700/696192.pdf.

81 Elliott Mai, *RAND in Southeast Asia: A History of the Vietnam War Era* (Santa Monica: RAND Corporation, 2010), vii, https://www.rand.org/pubs/corporate_pubs/CP564.html.

82 Ibid., 231.

83 Daniel S. Greenberg, "IDA: University-Sponsored Center Hit Hard by Assaults on Campus," *Science* 160, no. 3829 (May 1968): 744–748, https://science.sciencemag.org/content/160/3829/744; and Office of Technology Assessment, "A History of the Department of Defense Federally Funded Research and Development Centers," 28.

84 Konrad Kellen, *A View of the VC: Elements of Cohesion in the Enemy Camp in 1966–1967* (Santa Monica: RAND Corporation, 1969).

85 John Ponturo, "Analytical Support for the Joint Chiefs of Staff: The WSEG Experience, 1948–1976," Institute for Defense Analyses, July 1979, https://apps.dtic.mil/dtic/tr/fulltext/u2/a090946.pdf.

86 Ibid., 130.

87 Founding participants were the California Institute of Technology, Case Institute, Massachusetts Institute of Technology, Stanford University, and Tulane University. Others were added in subsequent years—the University of California, University of Chicago, Columbia University, University of Illinois, University of Michigan, Pennsylvania State University, and Princeton University—to make up a total of twelve members.

88 While the quality of research at FFRDCs has varied over time and across issue areas, some have done truly pathbreaking science.

89 Seth G. Jones, "Improving U.S. Counterinsurgency Operations," RAND Corporation, 2008, https://www.rand.org/pubs/research_briefs/RB9357.html; and Jonathan P. Caulkins, Peter Reuter, Martin Y. Iguchi, and James Chiesa, *How Goes the "War on Drugs"?: An Assessment of U.S. Drug Problems and Policy* (Santa Monica: RAND Corporation, 2005), https://www.rand.org/content/dam/rand/pubs/occasional_papers/2005/RAND_OP121.pdf.

90 JASON Program Office, "Lifetime Extension Program (LEP) Executive Summary," RAND Corporation, September 9, 2009, https://fas.org/irp/agency/dod/jason/lep.pdf.

91 Government Accountability Office, "GAO's Agency Protocols," U.S. Government Accountability Office, October 2004, https://www.gao.gov/new.items/d0535g.pdf.

92 UN Department of Global Communications, "UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis," March 28, 2020, https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19.

93 The International Fact-Checking Network (IFCN) at the Poynter Institute maintains a searchable database of false claims identified by their network of independent fact-checking in more than seventy countries around the world along with other tools for journalists. See "Fighting the Infodemic: The #CoronaVirusFacts Alliance," The Poynter Institute, accessed May 28, 2020, https://www.poynter.org/coronavirusfactsalliance/. Beginning in late March 2020, ESOC published regular updates to a structured database on coronavirus-related misinformation narratives in more than twenty languages. See Jacob N. Shapiro and Jan Oledan, "COVID-019 Disinformation Data," Empirical Studies of Conflict at Princeton University, accessed May 28, 2020, https://esoc.princeton.edu/files/covid-019-disinformation-data. And Agence France Press put up a website providing detailed reporting on hundreds of false claims. See "AFP Covid-19 Verification Hub," Agence France Press, May 6, 2020, https://factcheck.afp.com.

94 "How Facebook Can Flatten the Curve of the Coronavirus Infodemic," Avaaz, April 15, 2020, https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/. On Facebook's response, see Joe Tidy, "Coronavirus: Facebook Alters Virus Action After Damning Misinformation Report," *BBC News,* April 16, 2020, https://www.bbc.com/news/technology-52309094.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org