DAY ONE PROJECT

A National Cloud for Conducting Disinformation Research at Scale

Saiph Savage
Cristina Martínez Pinto

Co-authors:
Shannon Biega
Luz Elena González
Claudia Flores-Saviaga

June 2021

Summary

Online disinformation continues to evolve and threaten national security, federal elections, public health, and other critical U.S. sectors. Yet the federal government lacks access to data and computational power needed to study disinformation at scale. Those with the greatest capacity to study disinformation at scale are large technology companies (e.g., Google, Facebook, Twitter, etc.), which biases much research and limits federal capacity to address disinformation.

To address this problem, we propose that the Department of Defense (DOD) fund a one-year pilot of a National Cloud for Disinformation Research (NCDR). The NCDR would securely house disinformation data and provide computational power needed for the federal government and its partners to study disinformation.[1] The NCDR should be managed by a governance team led by Federally Funded Research and Development Centers (FFRDCs) already serving the DOD.[2] The FFRDC Governance Team will manage (i) which stakeholders can access the Cloud, (ii) coordinate sharing of data and computational resources among stakeholders, and (iii) motivate participation from diverse stakeholders (including industry; academia; federal, state, and local government, and non-governmental organizations).

A National Cloud for Disinformation Research will help the Biden-Harris administration fulfill its campaign promise to reposition the United States as a leader of the democratic world.[3] The NCDR will benefit the federal government by providing access to data and computational resources needed to combat the threats and harms of disinformation. Our nation needs a National Cloud for Disinformation Research to foresee future disinformation attacks and safeguard our democracy in turbulent times.

Challenge and Opportunity

Disinformation is increasingly fomenting public distrust and impacting national security, election integrity, public health, and other critical U.S. sectors. The 7.2 million mentions of rumored antifa violence and 6.2 million mentions of the QAnon conspiracy theory on social media are believed to have contributed to the January 6th attack on the U.S. Capitol.[4] The Election Integrity Partnership (EIP) identified 639 distinct misinformation and disinformation campaigns related to the 2020 U.S election across 15 social-media platforms, 72% of which explicitly aimed to delegitimize the election.[5]

Deeper understanding of the mechanisms, scope, and impacts of disinformation campaigns are needed to address this pressing issue. However, disinformation research requires massive and expensive amounts of computational power and data. This limits the entities that can conduct disinformation research at scale to large technology companies (e.g., Google, Facebook, Twitter, etc.) that already have access to substantial computing resources and control the pipeline of user-generated data on widely used internet platforms.[6,7] Consider, for instance, a Twitter post suspected to contain covert disinformation. Relative to

[1] Stanford Law School. (2021). Policy Practicum: Creating a National Research Cloud. Course Catalog.
[2] U.S. Government Accountability Office. (2020). Federally Funded Research and Development Centers: Improved Oversight and Evaluation Needed for DOD's Data Access Pilot Program. GAO-20-272.
[3] JoeBiden.com. (n.d.). The Power of America's Example: The Biden Plan for Leading the Democratic World to Meet The Challenges of the 21st Century.
[4] Singer, P.W. (2020). Misinformation 2020: What the Data Tells Us About Election-Related Falsehoods. Defense One, November 5.
[5] Center for an Informed Public; Digital Forensic Research Lab; Graphika; Stanford internet Observatory. (2021). *The Long Fuse: Misinformation and the 2020 Election, 2021*. Election Integrity Partnership. V1.2.0.
[6] Jensen, B. (2021). How to Build a National Research Cloud. Stanford University Human-Centered Artificial Intelligence, February 23.
[7] Fowler, G.A.; Alcantara, C. (2021). Gatekeepers: These tech firms control what's allowed online. *The Washington Post*, March 24.

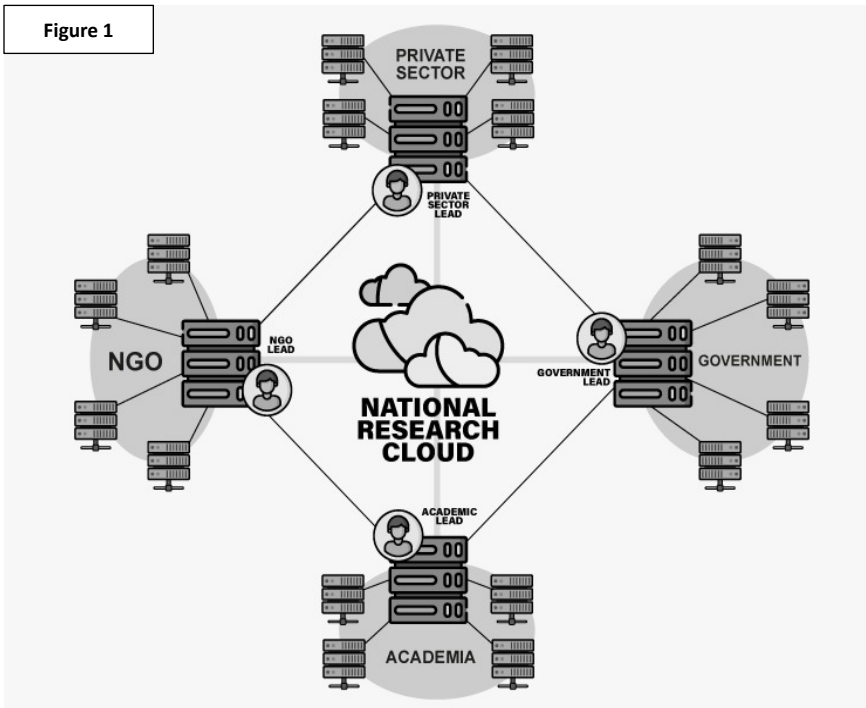
external analysts, Twitter can build a much deeper picture about how that post might relate to larger-scale disinformation campaigns being deployed across the platform by similar actors. The result is pervasive bias in much disinformation research. Moreover, limited visibility makes it difficult for the federal government to create national defense strategies against disinformation or to research the design of intelligent interfaces to combat the phenomenon. Part of the challenge is determining how best to share disinformation data and computational resources for stakeholders to study collectively disinformation at scale without compromising privacy, security, or proprietary interests.

Though big tech companies have made gestures towards addressing the disinformation problem (including Facebook's Social Science One and recent initiative for sharing data with select researchers,[8] as well as similar programs at Twitter[9]), these privately run efforts are insufficient. Company-led orchestration and oversight of data and computational sharing setups inevitably biases what is and is not studied. Centralized, company-led governance of information flows and disinformation research can also raise suspicion that voices not aligned with the interests of "Big Tech" are being censored.[10]

Plan of Action

We therefore propose that the Department of Defense (DOD) fund a one-year pilot of a National Cloud for Disinformation Research (NCDR) designed to democratize the study of disinformation. The NCDR will consist of a network of servers that will be readily available for stakeholders to use to conduct large scale disinformation research. The NCDR will also have a "data library'' that holds data to help researchers conduct their disinformation research (which is important as lack of data can limit and bias disinformation studies). Additionally, the NCDR will introduce a governance model to coordinate with different stakeholders to share computational resources, data, and facilitate collaborations across sectors and disciplines. The NCDR illustrates two core benefits relative to traditional approaches for conducting disinformation research: 1) scale, the ability to form and create research teams dynamically in response to research interests; 2) diversity, the ease with which stakeholders from diverse sectors and disciplines can be brought together to conduct disinformation research while having access to the computation and data that they need. Fig. 1 presents an

Figure 1



[8] Facebook Newsroom. (2020). New Facebook and Instagram Research Initiative to Look at US 2020 Presidential Election. August 31.
[9] Tornes, A.; Trujillo, L. (2021). Enabling the future of academic research with the Twitter API. Twitter Developer Blog, January 26.
[10] Tabick, B. (2021). Conservatives concerned about being silenced by big tech companies. KCRG News, January 16.

overview of our National Cloud and showcases how the research conducted on the NCDR could impact policy, the lives of citizens, and scientific knowledge.

We propose for the NCDR to be structured on the proven model of Federally Funded Research and Development Centers (FFRDCs) already serving the DOD.[11] The NCDR will provide a secure platform for sharing anonymized disinformation data and computational resources. The NCDR will also serve as a hub for fostering collaboration on disinformation research among technology companies, the federal government, NGOs, the private sector, and universities. Insights from NCDR-assisted research will enable the U.S. government to develop better strategies to combat disinformation, especially disinformation campaigns from foreign actors with malicious intent. For example, NCDR-assisted research could help us understand what types of actors tend to initiate disinformation as well as how and on what platforms they tend to do it. While research suggests that disinformation usually originates in more unconventional networks and then spreads via mainstream social-media platforms,[12] we do not know for sure. We also do not know the characteristics of the accounts that create and disseminate most disinformation. Better answers to these questions will help policymakers, law enforcement, tech companies, and others combat disinformation campaigns more effectively.

Other types of NCDR-assisted research could include tailoring intervention strategies to different groups.[13] With increased data access — and by working closely with large internet companies and their end-users — researchers could better study the effectiveness of specific interventions (e.g., certain fact-checking setups) across different platforms, topics, and audience demographics. Such strategies would bolster the fight against disinformation while reducing negative side-effects from anti-disinformation campaigns (e.g., sometimes when people get used to seeing fact checking interventions, they start changing their behavior for consuming news which can make them more susceptible to fall for disinformation when the fact checking intervention is not implemented. Cross-platform analysis of how these interventions affect user behavior will allow for the design of a more robust fact checking).

The idea for National Research Clouds has been gaining traction in the Artificial Intelligence (AI) space.[14] The concept is that by sharing data and computational resources via an internet-enabled network, National Research Clouds will make it far easier for academics, government agencies, and private-sector companies to research and train AI systems. The National AI Research Resource Task Force of 2020[15] lays out a roadmap for creating a national cloud and computational resource pool to advance AI. We propose a similar roadmap, additionally inspired by President Obama's Cybersecurity National Strategy (CNAP)[16] of 2016, for using a national cloud to conduct large-scale disinformation research.

The one-year pilot to lay the foundation for — and start studying applications of — a closed, decentralized, and nonpartisan National Disinformation Research Cloud (NDRC). During this one-year effort, the pilot should (1) establish governance principles for the NDRC; (2) build a first iteration of the actual cloud platform; and (3) facilitate the use of the cloud by a range of stakeholders to conduct disinformation

[11] Wanless, A.; DeCaires Gall, K.; Shapiro, J.N. (2021). Using an Old Model for New Questions on Influence Operations. Freedom to Tinker, January 27.
[12] Freelon, D.; et al. (2020). Black trolls matter: Racial and ideological asymmetries in social media disinformation. *Social Science Computer Review*: 1–19.
[13] Pasquetto, I.V.; et al. (2020). Tackling misinformation: What researchers could do with social media data. *The Harvard Kennedy School Misinformation Review*.
[14] Stanford University Human-Centered Artificial Intelligence. (2020). National Research Cloud Call to Action.
[15] Lohr, S. (2020). Universities and Tech Giants Back National Cloud Computing Project. *The New York Times*, June 30.
[16] The White House. (2016). FACT SHEET: Cybersecurity National Strategy. February 9.

research. Progress towards each of these goals will build on work to date in data collaboratives[17] and data archives,[18] which have created multidisciplinary shared research resources. Progress will also incorporate lessons learned from how these efforts have started to comply with legal and ethical requirements via new differential privacy mechanisms, as well as lessons from National AI Research Clouds.[19] The overarching goal is the development of a National Disinformation Research Cloud that motivates multi-stakeholder participation[20] and democratizes the study of disinformation.

We recommend that the cloud pilot be managed by a governance team responsible for recruiting and engaging new stakeholders who will contribute computational resources and disinformation data to help build cloud capacities. The governance team will oversee how disinformation data between stakeholders will be shared and studied and will motivate multi-stakeholder participation. As part of this work, the governance team will draw on the long-lived data archives for knowledge reuse that have been housing multidisciplinary data for 15 years and counting.[21] The governance team should be led by Federally Funded Research and Development Centers (FFRDC) already serving the DOD.[22] A particularly valuable contributor to the NDRC would be the Software Engineering Institute at Carnegie Mellon University,[23] an FFRDC that could facilitate the study of the technical aspects of the cloud in a way that prioritizes cybersecurity and privacy. The governance team should also include stakeholders from different sectors (academia, industry, NGOs, and government) to further facilitate collaboration, advising, and the general success of the cloud.

The following sections provide more detail on the NDRC design, governance, users, and data inputs.

NDRC Design

The NDRC should comprise computational resources from a network of different stakeholders across industry, academia, government, and NGOs. Stakeholders will apply to be a part of the NDRC and will be expected to share computational power, contribute data, and collaborate on research in exchange for access to resources contributed by other NDRC participants. Stakeholders could apply to be part of the NDRC through an online form, via which they would indicate what resources they could offer to the NDRC and what they expect from the collaboration in return. We expect that the governance team will work with each stakeholder to determine what constitutes an acceptable contribution.

In the year-long pilot we expect a minimum of a dozen different stakeholders from different sectors to participate in the NDRC. As the NDRC reaches maturity we expect that thousands of different stakeholders across the US will be part of the national cloud (including different NGOs, small businesses, universities, and governments who will all benefit from being able to use the NDRC to conduct disinformation research.) Each node in the NDRC network will represent the computational resources that a stakeholder has shared with the network. Stakeholders will be able to use one or more nodes simultaneously to conduct large-scale disinformation studies (i.e., more computational resources than they would have access to working independently).

[17] GovLab. (n.d.). Designing a Data Collaborative. Data Collaborative.
[18] Borgman, C.; Scharnhorst, A.; Golshan, M. (2018). Digital Data Archives as Knowledge Infrastructures: Mediating Data Sharing and Reuse. *Journal of the Association for Information Science and Technology*, 70(8): 888–904.
[19] Lohr, S. (2020). Universities and Tech Giants.
[20] Farmer, R. (n.d.). Making Computer Science Education Universal for All Students. Day One Project.
[21] Borgman, C.L.; Scharnhorst, A.; Golshan, M.S. (2019). Digital data archives.
[22] National Science Foundation. (2021). Master Government List of Federally Funded R&D Centers.
[23] Carnegie Mellon University. (n.d.). Software Engineering Institute.

Examples of pressing research topics that stakeholders could focus on during the pilot phase include cross-platform studies on how Russian influence campaigns are targeting African Americans,[24] how disinformation campaigns evolve over time across platforms, and what is the best "vaccine" to prevent viral disinformation operations.

NDRC Governance

The NDRC will be managed by a governance team that defines policies needed to establish and entrench the NDRC, ensure that it is used efficiently, and coordinate participation across stakeholders from different sectors and institutions. The governance team will define which stakeholders are invited to participate in the cloud, the type and amount of computational resources that each stakeholder will allocate to this network, and the types of transactions for which various computational resources will be used (e.g., to store disinformation data or to conduct cluster-based pattern analysis of large disinformation datasets).

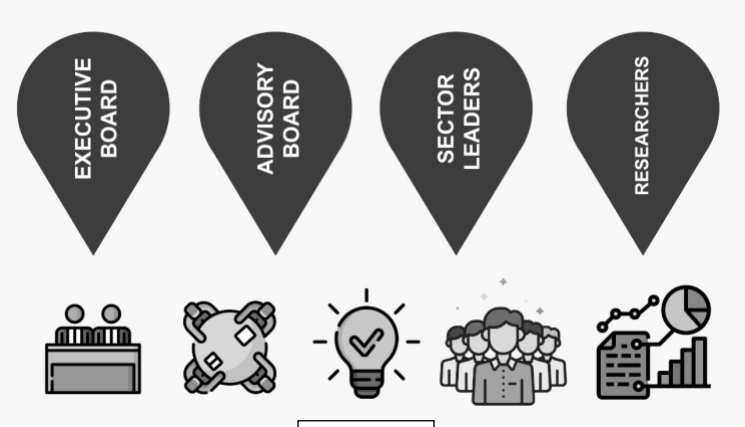


Figure 2

This section outlines a suggested governance model for the NDRC, one inspired by a similar model we (the authors of this memo) worked with the federal government of Mexico to implement for a National Blockchain Network in that country.[25] This model calls for a governance team comprised of an Executive Board, an Advisory Board, and leaders of sector-specific stakeholder and researcher networks.

Executive Board

The Executive Board will be the NDRC's strategic arm. It will oversee execution of the cloud's policies and guarantee that the cloud's computational resources are used effectively and ethically while respecting privacy concerns. The Executive Board will include two representatives each from industry, academia, government, NGOs, and FFRDCs with relevant experience. Ideally, one of these representatives will have expertise in disinformation policy[26] and the other will have expertise in the technical aspects of disinformation campaigns.[27] The **policy representative** will have expertise in areas such as legislating, foreign affairs, news-media operations, and privacy compliance. The policy representatives will help the Executive Board select research proposals to approve by weighing in on which proposals are likely to deliver greatest public benefit. The **technical representative** will have expertise in areas such as big data, differential privacy, and advanced computation. The technical representatives will help the governance team determine whether a proposed contribution of data and computational resources should be deemed sufficient for NCDR membership. The technical representatives will also help ensure that all

[24] Švedkauskas, Ž.; Sirikupt, C.; Salzer, M. (2020). Russia's disinformation campaigns are targeting African Americans. *The Washington Post*, July 24.
[25] Savage, L.; Eber, B.; Savage, S. (2019). *Blockchain for Governance and Civic Participation in Mexico*. White paper.

[26] See FAQ for more detail.
[27] See FAQ for more detail.

prospective NCDR participants have the technical capabilities to adequately function as nodes inside the cloud. Finally, technical representatives will recommend upgrades and improvements to NCDR technical infrastructure as necessary and will ensure that the NCDR's computational and data resources are being used efficiently and effectively.

Executive Board members will be responsible for reviewing and approving the disinformation-research projects that stakeholders propose, promoting use and adoption of the cloud, and recruiting future members. The members of the FFRDC will be the initial drivers of the Executive Board. The Executive Board will designate an Executive Secretary in charge of coordinating meetings and following up on participation agreements.

During its regular meetings, the Executive Board will make decisions about cloud access and governance (e.g., when different stakeholders will have access to different computational resources), identify research priorities, and select other members of the governance team (e.g., the Advisory Council and sector leaders). We expect that there will be about three regular meetings per year. Additional special meetings could be held as necessary, contingent on the consent of at least 80% of the Executive Board.

Advisory Council

The Advisory Council will be a group of experts responsible for advising the governance team on the NDRC's structure, function, and research priorities. Membership in the Advisory Council will be open to anyone from an academic institution, research center, industry, NGO, or government with relevant expertise.

Sector Leaders

Sector leaders will be individuals responsible for recruiting and engaging stakeholders from a particular sector. At a minimum, there should be one leader each for the following four sectors: academia, industry, government, and NGOs. The leader of each sector will be nominated by other NDRC participants from that sector and confirmed by the Executive Board. Functions of sector leaders will include:

- Helping connect new nodes to the cloud, ensuring that they adhere to technical standards and comply with privacy protections and ethics codes.
- Collecting, analyzing, and selecting promising research proposals from their sector for final review by the Executive Board.
- Monitoring performance of computational resources and data from their sector.

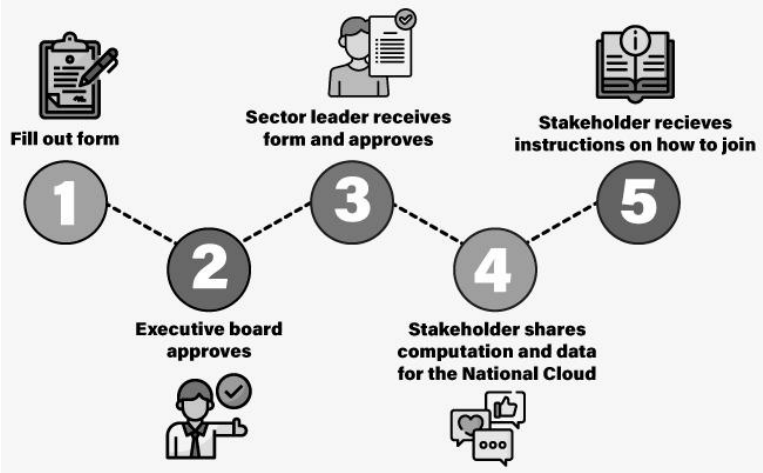
NDRC Users

"NDRC users" refers to institutions and individuals approved to conduct disinformation research on the national cloud. Because the NDRC will be closed, only those approved by the governance team to join will be able to access its data and computational resources. Access will be granted on an as-needed basis according to research proposals users submit to sector leaders (subject to approval by the Executive

Board). Each proposal will need to specify the overall goal, methodology, requisite data and computational resources, broader impacts, and design and policy implications.

NDRC Data Library

Figure 3



The year-long NDRC pilot will explore two different mechanisms to ensure that the cloud is adequately supplied with data and it can be a data library for disinformation studies. These mechanisms are (i) subscription APIs, and (ii) targeted engagement with industry.

Subscription APIs

Commercially available APIs (i.e., "subscription APIs") will be used to collect initial data deposits from large technology companies. In this mechanism, the NDRC will leverage the APIs that large technology companies (such as Facebook[28] and Twitter[29]) are already offering to scientists for data scraping, as well as the APIs that companies such as Meltwater[30] have made available. Meltwater, the world's first online media-monitoring company, offers a vast range of APIs for collecting data from different sources. APIs from Meltwater alone will give the NDRC access to data from 15 different social-media channels (including access to all of Twitter's content), blogs, online comments, news articles, and product reviews.[31] Meltwater can also provide data for over 270,000 news sources and over 25,000 podcasts, and offers several different options for collecting data about TV and radio shows. The NDRC will be able to use these subscription APIs to provide participants with a rich data library to get research projects started.

It is important to note that data offered through subscription APIs are not necessarily designed for disinformation research. Subscription APIs from Facebook and Twitter are better suited for general-purpose research, while subscription APIs from companies such as Meltwater are better suited for public relations. The governance team will need to work closely with NDRC users to figure out whether and how subscription APIs can be deployed in a way that provides adequate data for various disinformation studies. These discussions will also help the governance team identify data gaps that may require targeted engagement with industry to fill (see next section).

Targeted Engagement with Industry

The GovLab, an "action research center" based at New York University, has outlined approaches that the NCDR could use to motivate large technology companies to share data currently unavailable via

[28] Clegg, N.; Chaya, N. (2021). New Facebook and Instagram Research Initiative to Look at US 2020 Presidential Election. Facebook Blog, August 21.
[29] Tornes, A. (2021). Enabling the future of academic research with the Twitter API. Twitter Developer Blog, January 26.
[30] Meltwater. (n.d.). Meltwater Developer Portal.
[31] Meltwater. (n.d.). About Meltwater.

subscription APIs. Specifically, work from the GovLab's "Data Collaboratives" suggests that the NCDR could motivate companies to share data by highlighting the following:

- **Reciprocity.** If companies voluntarily share data to help the federal government combat disinformation, the federal government is less likely to impose mandatory and burdensome data-disclosure policies on those companies.

- **Value of research insights.** A company that contributes data to the NCDR could benefit from NCDR research—research that the company might not have the bandwidth or the specialized expertise to conduct in house. For instance, NCDR research insights could help a company improve its user interface and its approaches to combating disinformation on the platform it runs.

- **Gains in public perception.** Companies often participate in corporate philanthropy because they have a vision of producing a greater social good,[32] as well as because they can leverage philanthropic activities in public branding.[33] A company could frame participation in NCDR as a type of corporate philanthropy since combatting disinformation is a public good. This in turn could improve the company's reputation and revenue.

We envision that the NCDR governance team will motivate industry participation and data sharing by highlighting these points to companies. This approach has worked in other sectors. The "Computer Science for All"[34] initiative and the Software Collaboratives[35] are examples of multi-stakeholder, social-good efforts where non-financial incentives drove large internet companies to participate and donate data and computational resources.

Another strategy the governance team could adopt to motivate industry participation and data sharing is to work with the White House Office of Science and Technology Policy (OSTP) to host a series of high-profile meetings with senior executives from large technology companies. Such meetings will better define the accountability of internet platforms when it comes to disinformation and will provide a forum for establishing strong public-private partnerships in the fight against disinformation.

Data Types and Storage

We expect that the NCDR will store its data resources in the same or similar formats to the formats of data provided via the subscription APIs of large tech companies. For example, Twitter's API provides developers and researchers with data in the machine-readable JSON data structure. JSON file formats can be especially efficient when working with large-scale data that contains hierarchical structures. Multiple hierarchical structures can be associated with online data. An online post might encapsulate "child" information about the "location" at which the post was generated. The location value in turn might encapsulate "child" information about the "latitude" and "longitude" of the location. The NCDR could update its JSON datasets to include within the structure of those datasets whether the data holds disinformation (either in the form of binary flags or with a probability measure that highlights how likely is the post to hold disinformation). Large technology companies have adopted similar approaches for managing and sharing disinformation data.[36] NCDR datasets could be stored in a MongoDB database,

[32] Juholin, E. (2004). For business or the good of all? A Finnish approach to corporate social responsibility. *Corporate Governance,* 4(3): 20–31.
[33] Muzellec, L.; Lambkin, M.C. (2009). Corporate branding and brand architecture: a conceptual framework. *Marketing Theory,* 9(1): 39–54.
[34] Farmer, R. (n.d.). Making Computer Science Education Universal for All Students.
[35] State Software Collaborative. (n.d.). About the State Software Collaborative.
[36] Twitter Transparency. (n.d.). Information Operations.

which is open source, cross-platform, and uses JSON-like documents with schemas. Advantages of using this type of database is that it is efficient in storing, processing, and accessing JSON-type documents.

Conclusion

Disinformation is a rapidly escalating threat in the United States. The January 6th attack on the U.S. Capitol was fueled in large part by disinformation, and disinformation continues to exacerbate polarization of American communities. Our nation needs a National Cloud for Disinformation Research (NCDR) to democratize the study of disinformation and strengthen anti-disinformation capabilities. The NCDR will provide national value and impact in the following ways:

- **Situational awareness and response.** The NCDR will facilitate investigations and research that improve understanding of demographics and sectors of people most susceptible to disinformation, as well as understanding of the platforms, actors, and message types that tend to originate disinformation campaigns. These insights will enable the federal government to design better, targeted response strategies. The NCDR could even enable "Disaster Map"-style initiatives that allow government agencies and NGO to clearly visualize where they should concentrate anti-disinformation efforts.

- **Knowledge creation and transfer.** The NCDR will grant a greater number and diversity of institutions and individuals access to disinformation datasets that are currently widely dispersed. This unprecedented level of access will accelerate study of possible correlations and causalities within the field of disinformation and will make it far easier to identify factors that facilitate the spread and amplification of disinformation. Precedent for this expectation comes from MIT's Laboratory for Social Machines' Electome Project,[37] which showed how accessing large-scale data from social-media platforms improved forecasting and reporting around the 2016 U.S. presidential election. LinkedIn has coupled its social-media data with economic data to study how people's job-seeking behavior is influenced by their socioeconomic level. The NCDR could similarly facilitate studies around disinformation that involve a wide range of different variables (e.g., how a person's socioeconomic status affects their likelihood of falling for certain disinformation campaigns or participating production of disinformation).

- **Design and delivery of public services.** NCDR data and research insights will enable government agencies to better design public services that address disinformation, as well as to establish evidence-based policies for fighting disinformation. Examples of public services could include Digital Educational programs (that could exist in the form of handbooks and social media advertising campaigns) to raise awareness for the responsible and critical use of online election information.

- **Prediction and forecasting.** NCDR data and research insights will improve predictions about how a disinformation campaign could impact society. Better predictions can help governments proactively focus anti-disinformation efforts on campaigns that pose the greatest threats.

- **Impact assessment and evaluation.** NCDR data and research insights will help governments and NGOs assess the results of their interventions and actions to address disinformation in society. Assessment results will support iterative improvement of anti-disinformation strategies.

[37] Heyward, A. (2015). Enter the Electome. Medium, December 28.

The NCDR should be managed by a governance team initially led by FFRDC affiliates, with participation of stakeholders from industry, academia, and NGOs. The governance team will manage the NCDR's technical infrastructure and will oversee sharing of data and computational resources. The governance team will also recruit participants, evaluate research proposals, and facilitate research partnerships. The NCDR will enable cross-platform, multi-stakeholder research initiatives that will significantly improve understanding of the scope and nature of disinformation campaigns in the United States and around the world. This in turn will enable the U.S. federal government and its partners to create better national defense strategies against foreign actors targeting Americans through disinformation.

Frequently Asked Questions

1. Does the NCDR build on existing examples of Research Clouds?

Our proposal for a National Cloud for Disinformation Research builds on existing Research Clouds such as the European Cloud Initiatives' Open Science Cloud (EOSC)[38] and the Franco-German GAIA-X initiative.[39] The latter is promoted as a "federated ecosystem of cooperation" to manage public problems from a multistakeholder perspective and enable computing power to develop better policies. Its Technical Architecture Report provides a framework for the core architecture, governance, operating ecosystem, security elements, and data-protection provisions of a Research Cloud.[40]

Our proposal also draws on the Stanford Institute of Human-Centered Artificial Intelligence's (HAI) proposal to create a National Research Cloud for AI. This proposal has been widely supported and has attracted interest from 22 of the top 30 computer-science universities in the country. The proposal emphasizes that if the United States is to maintain global leadership in AI, new partnerships between academia, government, and the private sector must be created to devote computational, data, and human resources to research and training of AI systems. The HAI proposal directly catalyzed the National AI Research Resource Task Force of 2020, which directed the federal government to (i) investigate the feasibility and advisability of a cloud-based platform for large-scale AI research, and (ii) create a roadmap for such a platform. Many elements of our proposal for a National Cloud for Disinformation Research are inspired by the HAI proposal.

2. How will the NCDR differ from existing Research Clouds?

As a dedicated platform for disinformation research, the NCDR will enable more key stakeholders to study disinformation at scale. The NCDR will house data from numerous large technology companies (which no cloud currently does), providing structured access to these sensitive data via differential privacy (a system for sharing information about groups while hiding information about individuals). The NCDR's shared platform and extensive data library will foster an inclusive environment for cross-sectoral collaboration. NCDR resources and insights from NCDR research will help the federal government effectively combat disinformation campaigns.

3. How much will the NCDR cost?

[38] European Commission. (2021). European Open Science Cloud: A New Paradigm for Innovation and Technology.
[39] GTAI. (n.d.). GAIA-X – Germany and France Create European Data Ecosystem.
[40] Eggers, G.; et al. (2020). *GAIA-X: Technical Architecture*. Berlin: Federal Ministry for Economic Affairs and Energy (BMWi).

Similar initiatives give an approximate sense of the investment that will be needed to create and maintain the NCDR. In the United States, about $3.1 billion was allocated to the Information Technology Modernization Fund under the Obama administration. The European Open Source Cloud resource allocation and investment is estimated at €6.7 billion over five years (of which the Horizon 2020 fund will supply €2 billion, with the remaining €4.7 billion supplied by a combination of public and private investment).[41]

Overall, we expect that the costs for the first-year pilot of the NCDR will be $668,136 USD. The breakdown of the costs are:

- Funding in the amount of $52,144 USD is being requested to defray the costs of the Principal Investigator (PI). The PI will be responsible for general oversight of the project, including researching, developing, and deploying the National Disinformation Research Cloud. She will also run user studies, write research papers, and prepare related courses about the proposal's research. She will dedicate 25% of her total effort (3 months) to this project.

- Funding in the amount of $172,000 USD is requested to support four PhD students at 100% effort (12 months) participating in this project. The PhD student will assist the PI with researching, developing, and deploying the National Disinformation Research Cloud, as well as running user studies, and writing research papers. In specific, two of the PhD students will focus on prototyping the National Disinformation Research Cloud. The third PhD student will be in charge of researching and implementing the governance model with the different stakeholders and oversee its deployment on the National Cloud. The fourth PhD student will lead the user studies of the cloud usages and the effectiveness of our National Cloud to conduct disinformation research.

- The amount of Fringe benefits, based on the salaries of the personnel listed above, equals $26,715 and was calculated at a rate of 26.0 % for benefits-eligible personnel ($13,557 USD) and 7.65% for graduate students ($13,158 USD).

- Tuition remission budget is 25% of total cost of the normal course load of 16 credits per student. Expense is calculated, in project year one, as cost per credit $1,674.75 USD multiplied by four credits per academic year per student (for a total of $6,667USD per 12-month student)- Total cost for four students is $26,797 USD.

- We are requesting $50,000 USD to cover server and computation costs to build an initial prototype of the National Disinformation Research Cloud. These servers will be used to host throughout the grant all the related disinformation data and to have the computation power to conduct large scale disinformation research. It is important to note that the components to build the servers will be under $5,000 USD, but when the servers are completed, they will be classified as equipment because their total value is over $5,000 USD.

- $101,040 USD will be used to pay six expert consultants in disinformation who will be actively participating in the Executive Board.

[41] European Commision. (2020). The European Cloud Initiative.

- Funding in the amount of $24,750 USD is requested for a subcontract with Federation of American Scientists (FAS) that will oversee that the disinformation research cloud addresses the needs and concerns of stakeholders from the U.S. Federal Government. The FAS will also ensure the participation of stakeholders from the Federal Government to use the research cloud to conduct research or collaborate with academics in research that can benefit the Federal Government in creating strategies against the threats and harms of disinformation. The Federation of American Scientists will receive $24,750 in year one of the proposed project. The authorized representative for the Federation of American Scientists has reviewed and endorsed their organization's participation in the proposed research.

- Indirect costs (which are $214, 690 USD) are calculated using DHHS's negotiated rate of 57% per University's rate agreement dated 08/27/20. Indirect cost base is Modified Total Direct Costs—Total Direct less equipment, participant costs, tuition and subcontract costs in excess of $25,000 USD.

4. How will the NCDR handle data privacy and research ethics?

The NCDR will be closed, meaning that only institutions and individuals approved by the governance team will be able to access its data and computational resources. Beyond this initial screening, the NCDR will focus on being as transparent and interdisciplinary as possible, while utilizing privacy-preserving technologies that are also secure and have different access control mechanisms. Similar to practices in data collaboratives[42] and data archives,[43] the NCDR will follow a philosophy that providing data access is not a pretext for privacy violations or erosions. We will aim for the disinformation data that is shared on the NCDR to be in general aggregated and anonymized data that follows strict rules to ensure privacy. As explained above, our Sector Leaders and the Technical profile in the Executive Board will play a key role in ensuring these data protections. Similar to the principles of data collaboratives, we argue that societal benefits (e.g., better understanding disinformation) cannot come at the cost of losing individual rights around privacy. The governance team will work with Institutional Review Boards and ethicists on a set of operating principles ensuring that NCDR research respects human rights and privacy law. The NCDR will also follow privacy and ethics best practices established by other data collaboratives[44] and data archives[45] that have created shared research resources involving sensitive data.

[42] Verhulst, S.; Young, A.; Srinivasan, P. (n.d.) An introduction to Data Collaboratives. Data Collaboratives.
[43] Borgman, C.L.; Scharnhorst, A.; Golshan, M.S. (2019). Digital data archives.
[44] Verhulst, S.; Young, A.; Srinivasan, P. (n.d.) An introduction to Data Collaboratives. Data Collaboratives.
[45] Borgman, C.L.; Scharnhorst, A.; Golshan, M.S. (2019). Digital data archives.

About the Authors

Dr. Saiph Savage is an Assistant Professor at Northeastern University, the director of the Civic Innovation Lab, and a fellow at the Center for Democracy & Technology. She was named one of the 35 Innovators under 35 by the MIT Technology Review. Saiph has helped federal governments adopt human-centered design principles and artificial-intelligence capabilities. Her work has been covered by the BBC and *The New York Times*. Saiph holds a bachelor's degree in Computer Engineering from the National Autonomous University of Mexico (UNAM), and a Ph.D. in Computer Science from the University of California, Santa Barbara (UCSB).

Cristina Martínez Pinto is a Senior Research Scientist at Dr. Saiph Savage's Civic Innovation Lab. She is also the Founder and CEO of the PIT Policy Lab, working at the intersection of Public Interest Technology and agile policymaking. She has worked as a Digital Transformation Consultant at the World Bank, led C Minds' AI for Good Lab, and co-founded Mexico's National AI Coalition IA2030Mx. Cristina holds a Master's in Public Policy from Georgetown University and a B.A. in International Relations from the Tec de Monterrey. She is a member of the World Economic Forum (WEF) Global Shapers community.

Shannon Biega is a junior at West Virginia University, majoring in Computer Science and Spanish with an Area of Emphasis in Cybersecurity. She works with Dr. Saiph Savage as an undergraduate research assistant. Shannon has been specializing in cybersecurity, disinformation, and techno-authoritarianism. She is also a strong advocate for women in science, technology, engineering, and math (STEM), and is passionate about using her knowledge and experience to help others reach their full potential, especially rural women and Latinas.

Claudia Flores-Saviaga is a Fellow at Facebook Research and Ph.D. student at Northeastern University. She hold a master's degree in Information Technology from Carnegie Mellon University. Claudia's research involves the areas of artificial intelligence, crowdsourcing, and social computing. She is interested in understanding how "bad actors" organize misinformation and propaganda messages, and how other citizens organize to debunk manipulative messaging campaigns. She is applying this knowledge to design intelligent systems that can fight disinformation at scale. She started her exploration of online spaces analyzing how political trolls were organizing during the 2016 U.S. presidential elections. Her research has been covered by the Associated Press, Newsweek, BuzzFeed, El País, and Slate.

Luz Elena Gonzalez is a visiting junior researcher at Dr. Saiph Savage's Civic Innovation Lab and also works at the PIT Policy Lab. Luz Elena specializes in International Development Cooperation with a focus on technology policy. She is interested in the intersection of data science and public policy, as well as in advancing ethical technology design to create more inclusive, sustainable, and resilient cities. She has worked as a consultant and project manager in the public sector. She has a B.A in International Relations from the Tec de Monterrey.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.

The Day One Project offers a platform for ideas that represent a broad range of perspectives across S&T disciplines. The views and opinions expressed in this proposal are those of the author(s) and do not reflect the views and opinions of the Day One Project or its S&T Leadership Council.