Leveraging Publicly Available Information to Identify International Partnership Opportunities

Margaret Stanley

Prepared for United States Cyber Command

Applied Policy Project
Batten School of Leadership and Public Policy
University of Virginia
April 2022

Table of Contents

Acknowledgments

I would like to thank Professor Kirsten Gelsdorf for her guidance and willingness to lend her support throughout this process. Special thanks to John Robinson for his advice and help in connecting me with my client.

I would also like to thank U.S. Cyber Command, my sponsor, and everyone else who has provided their support to this project. I value the time that they have lent to my efforts tremendously, and I have appreciated the opportunity to hear their insights.

Disclaimer

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

Honor Pledge

On my honor as a student at UVa, I have neither given nor received unauthorized aid on this assignment.

UNIVERSITY of VIRGINIA | FRANK BATTEN SCHOOL of LEADERSHIP and PUBLIC POLICY

Cover page image sourced from Defense Visual Information Distribution Service. Graphics by Petty Officer 2nd Class William Sykes.

Client Overview

U.S. Cyber Command, or USCYBERCOM, defends Department of Defense (DoD) information systems, the defense industrial base and other contractors working for the DoD throughout the U.S. and the world, critical infrastructure, and U.S. elections from cyber-attacks. USCYBERCOM targets nation states and "hacktivist" groups used as proxies for foreign governments, as well as individual hackers using tools like ransomware to target critical infrastructure. Unlike organizations like the Department of Homeland Security or the Federal Bureau of Investigation, USCYBERCOM has the authority to conduct offensive cyber operations but cannot conduct these operations within the confines of the territorial U.S. (USCC Sponsor, personal communication, November 9, 2021).

USCYBERCOM has determined a need to secure greater cooperation and partnerships abroad in its efforts to accomplish its mission. This Applied Policy Project aims to provide analysis that will ultimately contribute to a strategy for effectively leveraging publicly available information to gauge perception of the U.S. and identify international partnership opportunities.

Executive Summary

As adversary aggression in the cyber domain intensifies, identifying and securing international partnership opportunities has become increasingly important to USCYBERCOM's mission. Leveraging publicly available information (PAI) is essential to understanding foreign perceptions of the U.S., which is especially important as the U.S. competes for influence with China, Russia, and other states. Evaluating these perceptions will help USCYBERCOM identify opportunities for international partnerships.

While literature evaluating methods for analyzing PAI and measuring perception supports key insights into these processes, available evidence on the effectiveness of these methods is somewhat limited. Use of these methods by major entities in the private, public, and non-governmental sectors does, however, suggest their efficacy. Primary mechanisms include surveying or polling to gauge foreign perception and use of artificial intelligence to analyze large volumes of PAI. Artificial intelligence could be especially promising as USCYBERCOM looks to analyze large volumes of information, much of which is not in English. USCYBERCOM might look to other entities, both private and public, for their analysis and insights into these processes. In doing so, analysts might also consider refining their models for gauging perception and look to less conventional sources to supplement their work.

Based on analysis of available literature, this report evaluates four policy alternatives:

1. Collaborate with another federal entity specializing in analysis of PAI in an information-sharing initiative
2. Pay a company to collect and analyze PAI on USCYBERCOM's behalf
3. Hire more personnel to analyze PAI and available open-source intelligence for insights into foreign perceptions of the U.S.
4. Partner with an academic institution that can leverage artificial intelligence to analyze PAI

After assessing each alternative on its expected feasibility, effectiveness, and cost, this report recommends that USCYBERCOM pursue Alternative 4. Given the policy window opened by the command's Academic Engagement Network, this alternative is estimated to be both feasible and effective. Several factors should be considered in implementing this recommendation, including identification of the partner institution, stakeholder perspectives, potential challenges, and best practices as observed through analysis of similar programs.

Introduction

As part of its efforts to identify and secure international cyber partnerships, USCYBERCOM has identified the need to better understand global perception of the U.S. by leveraging publicly available information. This project aims to contribute analysis in support of the command's long-term ability to achieve that goal. After reviewing relevant background information regarding the value and challenges of working with publicly available information, the importance of perception, and the significance of identifying and securing partnerships to USCYBERCOM's mission, the report discusses the costs and consequences of failing to adequately address the issue of interest. Applying takeaways from relevant literature, it then reviews four potential policy alternatives and recommends that USCYBERCOM partner with an academic institution on application of artificial intelligence. Finally, the report considers different aspects of implementing this alternative and briefly reflects on the importance of the issue and the proposed policy response.

Problem Statement

Since 2003, at least 228 significant cyber-attacks have targeted government agencies, defense and technology companies, and other major businesses in the United States, with the frequency of attacks against the U.S. and other countries increasing by 3,100 percent over the last two decades (*Significant Cyber Incidents | Center for Strategic and International Studies*, 2021). **To meet the global nature of this threat, U.S. Cyber Command has identified the need to leverage publicly available information to better understand perception of the U.S. and recognize opportunities for cyber cooperation.**

Background

Effectively leveraging publicly available information (PAI) is key to USCYBERCOM's ability to understand other states' perceptions of the U.S., its military, and its international activity. Awareness and understanding of these perceptions facilitate identification of countries that may be open to coordinating cyber efforts with the U.S. military. Identifying and securing these partnerships will be important for strengthening USCYBERCOM's long-term capacities and the command's ability to achieve its mission objectives. This section of the report reviews the value and challenges of working with PAI, the significance of the perceptions that PAI can help uncover, and the importance of partnership opportunities to USCYBERCOM's work.

Leveraging Publicly Available Information

PAI is information available or accessible to the public.[1] Sources of PAI include the Internet, media, public government data and information, professional and academic publications, commercial data, gray literature, and technical data (Wicker, n.d.). The ability to leverage this information is key to understanding how other states perceive the U.S. and identifying which countries are likely to be willing to partner with USCYBERCOM on international cybersecurity initiatives.

PAI analysis poses numerous challenges that can hinder analysts' ability to study it and draw relevant conclusions. The world's ten most spoken languages account for just under 50 percent of the global population (Lane, 2021; *World Population Clock*, 2022), and less than 5 percent of the world's population speaks English as a native language. Accordingly, most PAI is not written in English. The cultural and linguistic variety of PAI that analysts must contend with is a major challenge in processing and analyzing it (Chapman, 2020), especially when doing so with limited resources and a primarily English-speaking workforce.

The volume of PAI and the velocity at which it is produced daily also presents challenges to analysts. These factors have overcome a human's capacity for locating and analyzing relevant data, and analysts experience information overload (Wicker, n.d.). According to estimates, there will be over two hundred zettabytes of data in cloud storage by 2025 (Cobwebs Technologies, 2022).[2] This is largely driven by the proliferation of PAI across Internet sources like social media. A 2020 survey conducted among thirty-four countries showed that more than half of people in thirty-two of the countries reported using the Internet at least occasionally or owning a smartphone, and a majority of respondents in most of the countries reported using social media (Schumacher & Kent, 2020).

[1] The Department of Defense defines "publicly available information" as "Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public (Department of Defense, 2016)."

[2] Two hundred zettabytes are equal to 200,000,000,000,000,000,000,000 bytes (Cobwebs Technologies, 2022).

Why Perception Matters

Leveraging PAI is critical for understanding foreign perceptions and the geopolitical landscape. The perception that foreign publics and their governments have of the U.S. can help explain their past, present, and future behavior toward the U.S. (Magu, 2013, p. 127). A state's perception of the U.S. will determine its willingness to partner with the U.S. and its military on strategic operations. While the opinions of leadership elites in many countries determine their willingness to engage with the U.S. as a strategic partner, popular attitudes toward the U.S. have at least some influence over the behavior of even the most authoritarian regimes. These attitudes' impact on more moderate and democratic states can be significant (Cordesman, 2021a).

Global opinion of the U.S. is emerging as an essential form of competition between it, China, and Russia. The U.S.'s success in its competition with China and Russia, as well as other states like North Korea and Iran, depends largely on how states perceive it and their perception of the U.S. as an ally. Especially as adversaries like China gain on the U.S. in their economic and military strength, the U.S.'s ability to pursue its national interest abroad will not only depend on maintaining American military and economic strength but also on those perceptions (Cordesman, 2021b).

Fluctuation in foreign perception of the U.S. in recent years warrants pursuit of greater insight into foreign attitudes toward the U.S. and factors influencing those attitudes. This will be especially important as the U.S. seeks influence and partnerships in regions where it competes most directly with China and Russia, including Central Asia, the Indian Ocean region, Southeast Asia, the Middle East and North Africa, and sub-Saharan Africa (Cordesman, 2021b).

Importance of Identifying and Securing Partnerships

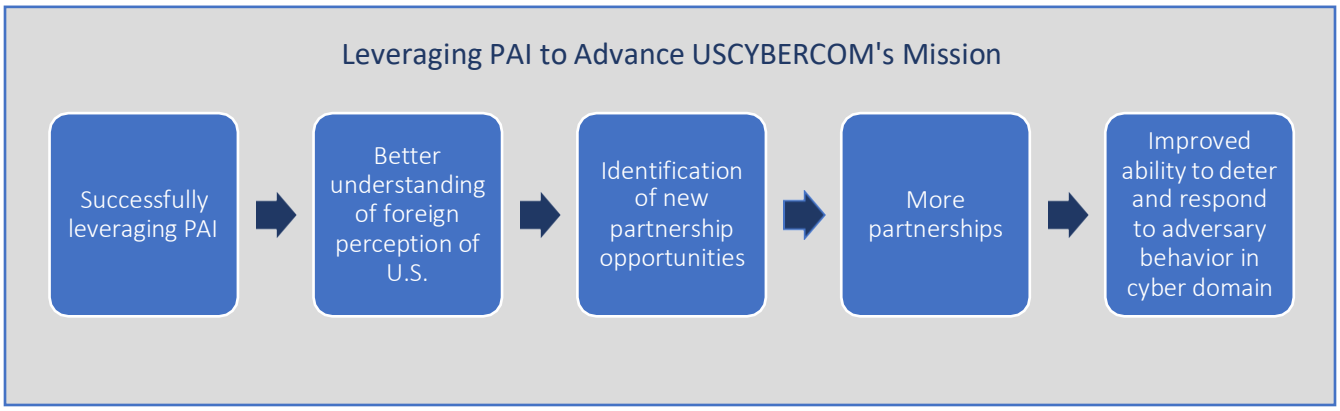
As attacks from nation-states like Russia, China, and other actors become more frequent and sophisticated, the importance of building new relationships that will support the U.S.'s cyber strategies with resources and insight will only grow.

Effectively leveraging PAI to produce actionable intelligence that provides insight into potential partner countries is important for USCYBERCOM's ability to accomplish its broader objectives and mission. This is largely due to USCYBERCOM's limited resources. USCYBERCOM's Cyber Mission Forces currently include roughly five to six thousand personnel, which are low-density and high demand (Tomczak et al., 2021). U.S. military officials have stated that future cyber initiatives should entail close coordination with U.S. allies and partners because USCYBERCOM's resources are so limited (Tomczak et al., 2021).

Cyber partnerships lend logistical support to U.S. cyber strategies. Defending against cyber-attacks requires that actual people gather information on an adversary, analyze it, and reconstruct the adversary's security environment in order to plan counterstrategies. Rehearsing exercises and missions, experimenting, certifying, assessing, and developing cyber strategies and tactics are labor- and resource-intensive (Myauo, 2016, p. 22–23; Sood & Enbody, 2013).

Furthermore, securing the ability to leverage partner capabilities enhances American cyber operations by enabling stronger collective cyber capacities, expanded operations, and greater information sharing in pursuit of partners' mutual interests (U.S. Department of Defense, 2018, p.2-

5). A greater number of analysts with regional expertise are more likely to spot attempted cyber-attacks as they are happening, allowing the U.S. and its partners to counter them quickly and prevent damage to national security and economic interests. These factors motivate policymakers' pursuit of greater insight into opportunities for international cyber cooperation.



Broader Security Context and Consequences

Failure to effectively leverage PAI to identify cooperation opportunities will limit USCYBERCOM's ability to find and secure international partnerships. This will contribute to continued strain on USCYBERCOM's resources, as well as diminished ability to deter adversaries' intensifying aggression in the cyber domain and mitigate related damage to national security and economic interests.

Intensifying Security Environment

An intensifying cyber environment adds a sense of urgency to identifying and securing international partnerships. Major cyber-attacks against the U.S., as well as other nations around the world, grew significantly more common in 2020 as the pandemic surged across the globe (Perrett, 2021). The number of attacks has continued to trend upward in 2021, with 22 significant cyber-attacks against the U.S. occurring so far this year (*Significant Cyber Incidents | Center for Strategic and International Studies*, 2021). Countries across the world have seen similar increases in cyber threats, with many of the most damaging international incidents occurring in the last five years (Ang, 2021). The increase in attacks perpetrated by nation-states or nation-state-supported actors is especially notable, with the number of these incidents doubling between 2017 and 2020 (Scroxton, 2021).

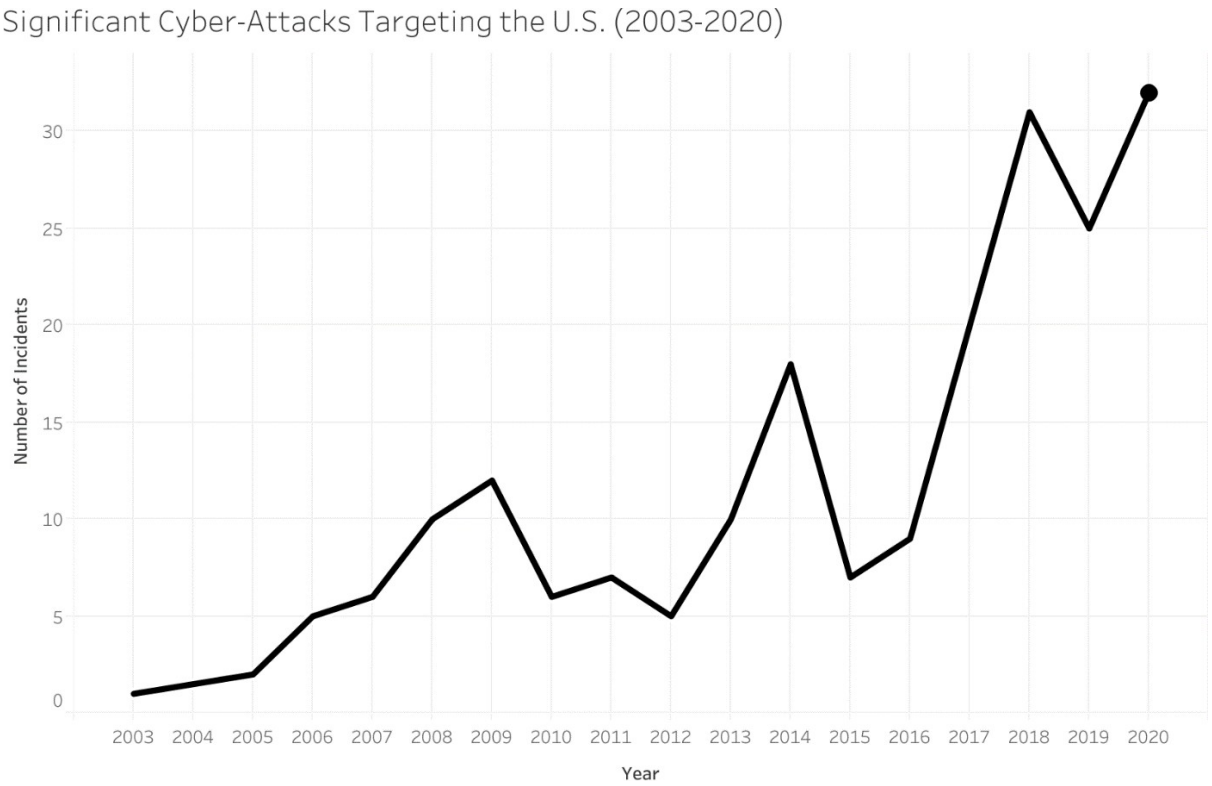


Figure 2 Graph shows trend over time in number of significant cyber-attacks targeting the U.S. between 2003 and 2020. "Significant cyber-attacks" are those targeting government agencies or defense and high-tech companies, as well as economic cybercrimes resulting in losses of over a million dollars. Data sourced from Center for Strategic & International Studies (2021).

As the frequency of major cyber-attacks has increased, these attacks have also become more sophisticated and harmful. Ten years ago, adversaries often worked through low-level attacks to steal data from U.S. stakeholders and disrupt systems. Nation-states and non-nation-state actors have since become more organized in their cyber operations. In the case of China, strategies that used to rely on phishing email schemes to commit intellectual property theft have since become more targeted and harder to detect, with elite satellite networks of contractors from companies and academic institutions now carrying out the work that People's Liberation Army units typically used to do (Perlroth, 2021).

This shift has not been limited to China. In December 2020, a single attack by Russia's leading intelligence agencies simultaneously hit the State Department, the Department of Homeland Security, Treasury Department, Commerce Department, Centers for Disease Control and Prevention, Justice Department, and DoD. Russian hackers stole data from the military, Intelligence Community (IC), and nuclear laboratories. U.S. officials highlighted that this attack notably diverged fromthe brute-force efforts and spear phishing that had routinely targeted the defense industrial establishment in the preceding two decades (Sanger et al., 2020).

This general trend has rapidly accelerated during the pandemic. A recent Microsoft report notes that cyber threat actors are now using techniques that make them significantly harder to detect and that threaten what should be the most secure targets. Attackers are actively developing new techniques for finding vulnerabilities in systems across the world, criminal hacking organizations are hiding more and more of their infrastructure in the cloud among legitimate services, and nation-states are compromising high-value targets with new reconnaissance strategies. Data shows that nation-state actors in particular are increasingly targeting entities and individuals involved in public policy and geopolitics who could influence official government policies, with Russia, Iran, China, and North Korea being the most active aggressors (Burt, 2020). INTERPOL analysis corroborates this assessment, pointing to a significant shift of targets from individuals and small businesses to major corporations, governments, and critical infrastructure (*INTERPOL, 2020)*. This trend has developed amid escalating international tensions and a rise in opportunities for nation-states to exploit systems as the pandemic has exposed vulnerabilities in countries' networks (Scroxton, 2021).

The DoD itself is navigating an increasingly threatening environment. In 2018, it saw 36 million attempts to breach its network via email daily as malware, viruses, and phishing schemes from a variety of actors attempted to gain access to military systems. Distributed denial-of-service attacks, some as fast as 600 gigabytes per second, have also targeted the Pentagon. As advancements are made in cloud computing, officials expect that these attacks will grow stronger (Konkel, 2018).

Costs and Consequences

Without the additional resources and manpower that cyber partnerships could provide, USCYBERCOM is less likely to prevent these cyber-attacks or catch cyberespionage campaigns as they occur. Left unchecked, adversaries' cyber campaigns against U.S. and allied countries' interests will lead to rising intellectual property theft and harm to stakeholder countries' economies, greater jeopardization of national security, and increasingly frequent attacks on political institutions and governance (Eftimiades, 2018). If adversaries are continuously able to infiltrate U.S. and partner countries' information systems, these countries could lose any military technological advantage to

hackers. China, for example, has been able to significantly expand its military capabilities in the last two decades largely because of its sustained cyberespionage campaigns against the militaries of the U.S. and its allies (Eftimiades, 2018).

In a recent interview, Brigadier General Matteo Martemucci of USCYBERCOM cited cyber-attacks on economic targets and large-scale theft of U.S. intellectual property as the greatest threat to the U.S. According to Martemucci, this activity costs the U.S. economy roughly $600 billion dollars each year, which is nearly equivalent to the DoD's annual budget (Ackerman, 2021). This scale of economic damage extends beyond the domain of individual American businesses and affects the American military apparatus, government, industry, and academia.

Literature Review

Scholarly literature has suggested new approaches to understanding and gauging perception. Availability of evidence on the effectiveness of specific methods of analyzing PAI and measuring perception is limited, with accessible literature largely limited to studies on related topics addressing the effectiveness of certain automated processes. Academic literature and information overviewing these methods and their use by non-governmental organizations, private sector companies, and other federal entities are somewhat more developed. This section reviews the primary mechanisms discussed in the literature and key takeaways for policymakers who want to work with PAI and gauge foreign perception.

Models for Gauging Perception

Models and methods for measuring perception differ across academic and industry domains. Practitioners operating in private sector marketing and academic fields like social psychology have focused empirical attention toward the factors and consequences of a country's image from their field perspectives. No model or measurement method has been widely established within the areas of public diplomacy and government relations, and a process for applying empirical approaches from other domains like marketing, public relations, and social psychology to these fields has not been widely determined. Instead, existing practitioner literature largely relies on aggregated indices and public attitude surveys (Buhmann, 2016b).

Drawing on concepts from national identity theory, attitude theory, and reputation management, scholars have attempted to answer this need with an integrative four-dimensional model accounting for functional, normative, aesthetic, and emotional dimensions of a country's public image. By incorporating perception of a country's overall competitiveness in various domains, integrity in terms of social and ecological responsibility, attractiveness regarding its culture and traditions, and feelings of liking and fascination that result from those dimensions, this approach lends toward a more nuanced interpretation of image that should be considered while attempting to gauge outside perceptions of the U.S. (Buhmann, 2016a; Buhmann & Ingenhoff, 2015).

Surveying

Surveying foreign publics is a primary mechanism for gauging foreign perceptions of states. Scholarly literature has historically used surveys and related methods as part of study methodologies, and some work has been done to analyze surveys themselves. The products of surveys conducted by major institutions are an important source of PAI for decisionmakers.

In the past, questionnaires have been successfully used to measure foreign student perceptions of the U.S. (Dalton, 1972). Analysis of major international surveys of nation branding and soft power underscores the utility of using surveys and analyzing available survey data in measuring foreign perceptions of nations (Buarque, 2019; Go & Govers, 2011; Reibstein, 2016). Major international surveys of nation branding include GFK's Anholt/GFK Nation Brands Index, Reputation Institute's Country RepTrak, FutureBrand's Country Brand Report, Portland's Soft Power 30, U.S.

News & World Report's Best Countries, the Institute for Government's Soft Power Survey, JWT's Personality Atlas, and the Good Country Index (Buarque, 2019).[3]

Many think tanks, companies, and other non-government entities use polling and surveying to measure foreign perception, including perception of the U.S. Pew Research Center, for example, conducts public opinion surveys in foreign countries. Working with local research institutions in a country of interest, Pew uses probability-based methods in in-person and phone interviewing to target non-institutional adult populations in the country, with sample sizes designed to yield at least one thousand interviews (Pew, 2022). Gallup similarly measures foreign attitudes using polling. For its World Poll, Gallup implements probability-based telephone and in-person surveys using a random-digit-dial method or nationally representative lists of phone numbers (Gallup, 2014). Afrobarometer conducts face-to-face interviews with randomly selected samples of 1,200 or 2,400 people in each survey country while working with national partners (Afrobarometer, 2022).

Some federal agencies collect and analyze information on foreign opinion using surveys and polling. The Office of Opinion Research in the State Department's Bureau of Intelligence and Research, for example, does so by conducting public opinion surveys and polls to measure foreign attitudes toward a variety of issues, including democratic transitions, ethnic and social relations, international security, governance, trade and economy, and other topics (Department of State, 2022). The Department of State has contracted these services from private companies in recent years (Department of State, 2018, 2021).

Artificial Intelligence

Artificial intelligence (AI) is another major mechanism for collecting PAI and leveraging it for insights into perception. Sources of PAI are large and growing quickly. While they can facilitate critical insights into the postures of adversaries and potential partners, datasets and other sources of PAI often contain large quantities of irrelevant, incorrect, and incomplete information. Prioritizing, verifying, and supplementing relevant information are critical, and the sheer volume of information available often means that these processes must be automated. Research has demonstrated the possibility of using automated processes to co-analyze disparate data sources, including in analysis of social media and other openly available sources to predict future threats to national security (Air Force, 2022). Private companies have also used AI and machine learning to analyze PAI for insights into perception (Cobwebs Technologies, 2022).

A 2014 study produced by a team of academic researchers analyzed the development and effectiveness of one such process, the Early Model Based Event Recognition using Surrogates (EMBERS), in predicting civil unrest events. EMBERS is a multi-model approach utilizing shallow linguistic processing prior to analysis of textual content and geocoding systems for tweets, news, and blog articles. Analyzing the application of EMBERS across ten Latin American countries, Ramakrishnan et al. (2014) observed significant regularities and high quality scores, with models showing selective superiority across countries. The technique's integration of several models proved largely effective (Ramakrishnan et al., 2014). Though this study did not focus specifically on analyzing PAI for insights into public perception of another state, predicting civil unrest requires

[3] Table with full list of surveys of interest can be found on p.297 in Buarque (2019).

analysis of PAI sources across social media platforms and other media sources that can provide insights into perceptions of the host country.

Other Methods

To assess the perception that foreign nationals and nations have of the U.S., one study has analyzed countries' signaling behavior through analysis of congruence voting with the U.S. at the United Nations General Assembly. While it is difficult to fully determine that correlation between voting and perception constitutes causation, the study's use of these variables suggests the potential value of observing variables correlated with certain sentiments and not just explicit expression of such sentiments (Magu, 2013).

Federal Entities

Some federal agencies specialize in analysis of PAI and open-source intelligence (OSINT), the product of that analysis. The Defense Intelligence Agency (DIA) is a lead DoD agency working with OSINT and information collected from social media, online material, commercial data sources, and other sources (Tau & Volz, 2021). The Central Intelligence Agency's Open Source Enterprise (OSE) also promotes the acquisition, procurement, analysis, and dissemination of OSINT and related products across the federal government (*Director of National Intelligence - Open Source Center*, n.d.). OSE OSINT analysts analyze public data sets and combine the information with analysis of classified sources (Konkel, 2016). While more specific information detailing the methods used by these entities is not publicized, their work with PAI could mean that they are already collecting information and producing analysis that would be useful in identifying potential partner countries.

Takeaways From the Literature

Recent scholarship suggests the need to develop a multifaceted understanding of the factors that shape perception of states. Review of relevant academic literature and analysis of methods used by different sectors highlights use of surveys and AI as primary mechanisms of measuring perception and exploitation of PAI. With the exception of select studies on specific AI tools, studies on the effectiveness of these methods are limited; however, their widespread use across academic, private, and public sectors suggests their efficacy.

Given the volume of PAI with which analysts must contend, automating the analysis process through use of AI or sourcing this analysis from another entity would likely prove more efficient than reliance on published survey data. Academic studies analyzing less traditional measures of perception, such as demonstrations of support for the U.S. in public international settings, suggest that these sources may also prove useful in supplementing perception-gauging processes where needed.

Criteria for Evaluation

Based on analysis of available evidence, this report proposes and assesses four possible alternatives that USCYBERCOM can implement in its efforts to better understand foreign perception using PAI. Alternatives are evaluated using the following criteria:

Feasibility

As a military entity, USCYBERCOM is limited administratively and politically in what it can implement, especially as the situation involves cooperation with outside institutions and agencies. Feasibility is estimated through consultation with USCYBERCOM officials, other current and former federal government officials, and individuals with experience in related private sector positions. Review of relevant literature and case study analysis also contributes to assessment of feasibility. Factors considered include expected institutional and stakeholder buy-in, possession of necessary authorities, existing processes in place to support the alternative, and policy context.

Effectiveness

Given that USCYBERCOM's resources are limited, the chosen alternative should be a productive use of those resources. Effectiveness is defined and estimated using analysis of the likely level of control and oversight that USCYBERCOM will have over each process, each option's estimated ability to overcome reasonably expected obstacles in order to achieve goals, and each option's likely ability to address and achieve USCYBERCOM's goals. Estimates of effectiveness are based on input from subject area experts with experience in related government and private capacities, gray literature analysis, and review of relevant case studies.

Cost

Federal budget allocations decided by the executive and legislative branches determine USCYBERCOM's resources for a given year's policy implementation, so estimated cost should be considered when comparing alternatives. This report estimates the cost of each alternative using publicly available cost estimates of analogous programs, available information on contract pricing, and standard pay scales and figures published by the federal government. The classified nature of USCYBERCOM's work makes it difficult to calculate opportunity cost, so opportunity cost is not explored at length in cost estimations; however, the time and resources that each alternative would take away from other Command efforts should also be considered by decisionmakers as they review different options.

Policy Alternatives

This report reviews four alternatives meant to improve USCYBERCOM's ability to leverage PAI and better understand perceptions of the U.S. for the purpose of identifying partnership opportunities. These alternatives include: 1) federal collaboration, 2) private sector partnership, 3) workforce expansion, and 4) academic partnership.

Alternative 1: Federal Collaboration

USCYBERCOM currently works with entities that specialize in collection and analysis of PAI, including DIA and OSE. This cooperation primarily consists of sharing intelligence on malicious cyber actors, tactics, and procedures (USCC Sponsor, personal communication, March 3, 2022). Utilizing these existing connections, this alternative entails partnering with one of these entities in a deliberate, specific, and consistent information-sharing initiative. The agency of interest would coordinate with USCYBERCOM to share relevant PAI and OSINT that is already being produced and that can provide insights into foreign perception, closing intelligence-sharing gaps.

Feasibility

The majority of experts with experience in federal government that were consulted for this report agree that this alternative is only somewhat feasible. Interviews with USCYBERCOM officials highlight regular meetings between senior level USCYBERCOM officials and relevant agencies to discuss various topics at the strategic level. Existing cooperation also includes analyst-level discussions on joint production, coordination, and collaboration initiatives (USCC Interviewee 2, personal communication, March 14, 2022; USCC Sponsor, personal communication, February 23, 2022; USCC Sponsor, personal communication, March 10, 2022; USCC Sponsor, personal communication, March 14, 2022). This alternative is also consistent with recent DoD efforts to actively improve processes for sharing data and information between its internal systems (USCC Sponsor, personal communication, March 10, 2022), which raises the likelihood of broader institutional support for the effort.

While it is clear that USCYBERCOM has the authority necessary to work with entities of interest to this alternative and that there is basis for broader institutional support for this type of initiative, bureaucratic and political hurdles would likely limit feasibility. Federal partnership initiatives require buy-in from all parties involved even when they already maintain an existing relationship, and it is unclear how USCYBERCOM could incentivize agency buy-in within this specific context. This could complicate efforts to implement this alternative, especially as agencies must agree on joint budgets, resource-sharing, and other logistical issues that are critical for cooperation and can lead to impasse (Interviewee 3, personal communication, March 13, 2022; Interviewee 5, March 14, 2022). When working with members of the IC, the need to ensure that USCYBERCOM adheres to federal regulations on intelligence collection by military entities also presents a potential hurdle that parties must jointly overcome (Interviewee 4, personal communication, March 14, 2022; USCC Interviewee 2, personal communication, March 14, 2022).

Effectiveness

To some extent, existing USCYBERCOM interagency efforts can serve as a model for predicting effectiveness. USCYBERCOM officials interviewed report collaboration efforts with DoD and other federal entities as effective and as achieving their intended purposes (USCC Sponsor, personal communication, March 10, 2022; USCC Interviewee 2, personal communication, March 14, 2022).

The need to compromise on goals, processes, and timelines is inherent to cooperation. USCYBERCOM may need to compromise on some of its priorities in order to account for the needs of partner agencies and maintain their investment in the project. This would mean that USCYBERCOM would likely not have as much freedom to directly pursue its own goals and shape the process to the extent that it would with other alternatives presented here (Interviewee 2, personal communication, March 13, 2022; Interviewee 3, personal communication, March 13, 2022). This would likely limit effectiveness regarding the command's ability to dictate priorities and control the process enough to ensure progress toward them. Furthermore, effectiveness will largely depend on maintaining participation by all parties and the degree to which shared responsibilities and goals are clearly defined and agreed upon early in the collaborative process (Interviewee 3, personal communication, March 13, 2022; Interviewee 4, personal communication, March 14, 2022). In the near future, the current geopolitical environment and ongoing crises like the Russian invasion of Ukraine will likely continue to monopolize the attention and resources of USCYBERCOM and any potential partner agencies. This will limit parties' ability to allot the time and discussion toward these requirements necessary for ensuring effectiveness.

Cost

Given the difficulty of determining exact cost values for personnel, facilities, capital, and other relevant costs within security-sensitive agencies in the IC and DoD, cost here is estimated using Congressional Budget Office (CBO) estimates of legislation proposing similar interagency coordination efforts across the federal government (Congressional Budget Office, 2019a, 2019b, 2021a, 2021b).[4] Analysis of CBO reports assessing the likely budget requirements of identified programs supports an estimation of this alternative's cost at roughly $462,500 per year.

[4] Programs identified based on determination of similar efforts regarding interagency coordination, involvement of information- and data-sharing, and estimated personnel and resource investment. See Appendix for more detailed overview of CBO-estimated bills and cost calculations.

Alternative 2: Private Sector Partnership

This option entails paying a private company that specializes in data analytics to collect and analyze PAI produced by countries of interest for USCYBERCOM. Depending on USCYBERCOM's internal workforce capacities at the time of implementation, it may choose to either have the company draw relevant conclusions for the command or do so in-house, with the private sector partner only providing information gathered and preliminary analysis. It should be noted, however, that the latter variation would take more time and resources away from other USCYBERCOM priorities and raise opportunity costs. Within this alternative, USCYBERCOM might also consider supplementing data analytics contracts by hiring companies to conduct surveys in countries of particular interest.

Feasibility

This option is highly feasible. USCYBERCOM currently has contracts with numerous companies in pursuit of a variety of Command objectives and has done so since its founding as part of its efforts to supplement its own limited workforce. Private sector partners provide support on hardware, software, cloud computing, personnel, and other services (USCC Sponsor, personal communication, March 10, 2022). USCYBERCOM thus already has at least some of the processes and relationships in place necessary for supporting this alternative. Given the current global context, this high degree of feasibility is more certain for some types of PAI collection and analysis than others. For instance, while federal entities like the Department of State and the U.S. Agency for International Development have demonstrated the feasibility of utilizing contracted surveying in foreign countries to gauge foreign public perception (Hysenagolli, 2019; Koré, 2016; *Who We Are*, 2017), current global conditions and the ongoing pandemic hinder in-person interviewing (Cordesman, 2021b). This is especially important to consider in certain regions that continue to suffer disproportionately under pandemic conditions, where logistical challenges to interviewing are likely to be especially concentrated. For the purposes of this report, this analysis assumes that, in implementing this alternative, USCYBERCOM would thus pursue services that do not entail in-person interviews.

Effectiveness

Assessment of effectiveness is based on analysis of the current market of companies that can provide services of interest and USCYBERCOM's likely access to the best expertise available, as well as its expected control over relevant processes. Companies of interest include those specializing in collection and analysis of PAI from the Internet and other media sources, as well as companies capable of adapting to and accommodating USCYBERCOM needs in order to be competitive for the necessary contract. Preliminary market analysis identifies multiple options, many of which have experience meeting the needs and processes of U.S. military customers (ATLAS, 2022; Booz Allen Hamilton, 2022; Deloitte, 2022; Everwatch, 2022; Leidos, 2022; Peraton, 2022; SAIC, 2022).

In a contractual context, USCYBERCOM would have sole decision-making power over partnership priorities and services requested (Interviewee 4, personal communication, March 14, 2022). When combined with the available market and USCYBERCOM's resulting diversity of choice in service providers, USCYBERCOM's sole control over services rendered and project design strengthens its ability to choose the company best-suited to the task and tailor this alternative to its needs. A majority of subject-matter experts consulted for this report noted that these factors support

determination of contracting with the private sector as likely to be highly effective. It should be noted that, while USCYBERCOM would have sole control over identifying the most beneficial contract, capacity for oversight and related ability to efficiently measure and maintain progress may not be as strong as with some other options that entail doing work in-house. This could somewhat limit effectiveness.

Cost

Analysis of State Department procurement forecasts for the type of data analytics contracts of interest to this alternative inform estimation of its cost. According to this data, the median cost of a contract of this nature would likely be roughly $7 million annually. Should USCYBERCOM choose to supplement this with targeted surveys, the cost of each additional survey contract would likely be between $250 thousand and $500 thousand per year (Department of State, 2018, 2021). The aforementioned competitive market of potential commercial contract partners raises the possibility of negotiating prices down, potentially lowering the cost of this alternative.

Alternative 3: Hiring Personnel

This option entails hiring more USCYBERCOM personnel to analyze PAI offering insights into foreign perceptions of the U.S. Rather than working consistently with other agencies specializing in PAI analysis and OSINT, this option would involve USCYBERCOM's implementation of methods and tools used by those entities for the specific purpose of drawing conclusions about foreign perception. This would also entail use of available information and analysis already being produced by entities like the Department of State. USCYBERCOM personnel would use these methods to analyze PAI, which would then help determine ideal countries with which to partner. Similar to the model used by the State Department, this alternative suggests assigning analysts to a "desk" that focuses on a particular region of interest to USCYBERCOM and delivers relevant conclusions to decision-makers once appropriate capacity has been constructed (U.S. Office of Personnel Management, 1958).

Feasibility

The majority of officials consulted felt that hiring more personnel to accomplish USCYBERCOM's goals of interest to this report is not currently feasible (USCC Sponsor, personal communication, March 10, 2022; USCC Interviewee 2, personal communication, March 14, 2022). Officials highlighted several factors that limit the feasibility of this alternative. Given the classified nature of the USCYBERCOM environment, these factors include the requirement that candidates for employment must be processed through lengthy background checks in order to obtain top security clearances (USCC Sponsor, personal communication, March 10, 2022; USCC Interviewee 2, personal communication, March 14, 2022).

Effectiveness

Because this process can be controlled by USCYBERCOM, its execution can be tailored to the command's priorities and existing capacities. It takes place in-house, strengthening ease of oversight that supports the likelihood that the project stays on track and meets performance goals (Interviewee 5, personal communication, March 14, 2022). USCYBERCOM's ability to set clear and informed guidelines from the beginning of this process and track progress toward benchmarks also lends toward this alternative's effectiveness.

The labor market context, however, may complicate this alternative's ability to optimize achievement of USCYBERCOM's goals. In a 2020 statement before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, USCYBERCOM Commander General Paul Nakasone noted that, even when the command can use financial incentives to retain personnel, they are not necessarily the most talented people available (Nakasone, 2020). The command's limited ability to compete with the private sector on the salaries and benefits that it can provide to candidates decreases the likelihood that it can attract the highest-performing candidates in the field (USCC Sponsor, personal communication, March 10, 2022). This would limit the effectiveness of this alternative.

Cost

Cost is estimated using standard government pay scales for the locality pay areas of Washington, D.C, Baltimore, and northern Virginia. Cost calculations assume that hired personnel would be onboarded as civilians within the higher end of the "Entry/Developmental", the "Full Performance", or the "Senior" pay band with the resulting range of estimated salaries and benefits based on associated GS/GG pay grades (Defense Civilian Intelligence Personnel System, n.d.). Assuming benefits would cost 40 percent of salary,[5] the cost per person is estimated to be between $72,282 and $191,479, with median predicted pay equaling about $131,880.[6] The higher end of this range is roughly consistent with DoD sample cost comparisons, which assess the full cost of a civilian at GS-14, Step 5 to the DoD at $164,570 per year (Department of Defense, 2020). Assuming this alternative would initially entail hiring five personnel to focus on regions determined by Command priorities, the total cost per year of this alternative is estimated at $822,850.

[5] Cost calculations estimated using following formula: Salary + (Salary * .4) = Total Cost including Benefits; range includes estimated cost of onboarding one person at GS/GG-9 Step 1 to GS/GG-13 Step 13 in Washington, D.C.-Baltimore-Northern Virginia locality.

Alternative 4: Analytics and Academic Partnerships

In January 2022, USCYBERCOM officials announced the command's new Academic Engagement Network (AEN), which formalizes partnerships with eighty-four universities in thirty-four states (Johnson, 2022). In line with the AEN's mandate to utilize analytic partnerships with academic institutions in support of USCYBERCOM's broader mission, this alternative entails students and researchers at one of these institutions using AI to analyze PAI and gain insight into foreign perception of the U.S. Whenever possible, analysis of perceptions would be conducted especially as they relate to potential cyber and military initiatives in countries of interest. With support and oversight from USCYBERCOM officials, researchers would work in an unclassified environment to analyze this information and synthesize relevant conclusions for consideration by USCYBERCOM decisionmakers. They would then use this analysis in their identification of international partnership opportunities.

Feasibility

Several factors make this alternative highly feasible. Rather than establishing an entirely new program, this alternative suggests adding a new component to an existing program that is actively being formed and can thus be altered to incorporate this initiative. It is consistent with broader USCYBERCOM efforts to prioritize partnerships with domestic U.S. sectors, including academia (Pomerleau, 2022). It is also consistent with the DoD's 2018 Artificial Intelligence Strategy, which calls for forming open AI missions with academic institutions while pledging stable funding for getting academics involved in DoD-relevant AI research and talent investment (Department of Defense, 2018). This increases the likelihood that there will be organizational buy-in at USCYBERCOM, as well as the broader DoD. Organizational investment is made even more likely by President Biden's decision to sign the William M. Thornberry National Defense Authorization Act for FY2021, which endowed the commander of USCYBERCOM with new authorities necessary for standing up personnel management programs that facilitate recruitment of experts in vital cybersecurity fields. This demonstrates high-level Executive support for related academic partnerships (Smith, 2021).

Analysis of a similar analytical academic partnership established by the National Security Agency (NSA), which is closely associated with USCYBERCOM and thus presents an especially pertinent case study, also predicts high feasibility. The NSA's Laboratory for Analytic Science (LAS) leverages academic data science expertise to encourage non-traditional approaches to intelligence problems (NC State University, 2022b). The LAS develops and applies new methods for analyzing data, and its "Sensemaking" initiative specifically focuses on collection and organization of information that turns insight into action (NC State University, 2022a, 2022d, 2022c). Operating since 2013, the LAS's continued work suggests that a similar initiative that leverages university researchers and AI analysis of PAI is highly feasible (Wilson et al., 2019), especially given that this alternative proposes a program that will focus on a single mission and issue.

Effectiveness

Research by Gupta et al. (2014) associates high levels of DoD satisfaction with the performance and effectiveness of certain categories of partnerships between the DoD and academia similar to that proposed here. Data collected via structured discussions with representatives from various DoD funding agencies and laboratories shows high levels of satisfaction among DoD laboratory leaders

and officials involved in these cooperation efforts (pp. 5–6). A 2019 survey of participants in the Intelligence Community Centers for Academic Excellence, a related program established in 2005 to encourage academic programs and professional development opportunities, also reported respondents' strong belief that the program achieves its objectives (Landon-Murray & Coulthart, 2020).

The success of the NSA's LAS again serves as a valuable reference here. While the LAS is a much more involved and complex endeavor than that proposed by this alternative, it employs academic researchers for intelligence analysis purposes. Its work involves AI and smaller tasks that more closely resemble the proposed program, making it a useful case study. Analysis of the LAS's progress since its founding in 2013 shows high levels of success based on several indicators. These include personnel testimony that underscores the significance of the LAS's continually approved and authorized operation and its effective integration of its mission and research personnel. These factors provide a benefit and capability not normally observed internally within its sponsoring agency. LAS personnel spoke to the initiative's notably immersive collaboration, integrated innovation, and facilitation of applying useful findings in mission spaces (Vogel & Tyler, 2019).

Cost

Cost estimates for this alternative are based on the cost of launching LAS. Each institution participating in that program received $1 million to $2.5 million in grants for the first year upon initiation of the program (Rockwell, 2014). The cost of conducting a similar program with one university for one year would be roughly $1.2 million to $3 million in today's dollars. To account for USCYBERCOM oversight, incorporating two USCYBERCOM personnel to oversee this project full-time would increase its cost by roughly $330 thousand to $420 thousand per year. This figure is based on DoD sample cost comparisons and assumes personnel would be civilians at GS-14, Step 5 or Military O-5 with twenty years of service experience (Department of Defense, 2020).

Outcomes Matrix

	Feasibility (.35)	Effectiveness (.45)	Cost (.2)	Total (Weighted)
Alternative 1	2	2	3	2.2
Alternative 2	3	2.75	1	2.4875
Alternative 3	1	2	2	1.65
Alternative 4	3	3	1.5	2.7

The rows above represent the policy alternatives addressed, and the columns show values representing alternatives' assessment according to the different criteria. Values represent the alternatives' estimated performance within each criterion relative to the other alternatives, with a higher value representing an assessment more favorable to USCYBERCOM. This matrix supports this report's recommendation that USCYBERCOM implement Alternative 4.

Recommendation

The AEN focuses on four lines of effort: future workforce issues, applied cyber research, applied analytics, and strategic issues (Johnson, 2022; Pomerleau, 2022). This report recommends that USCYBERCOM partner with an academic institution and its students as part of the broader AEN program. This partnership would be conducted in an effort to increase USCYBERCOM's access to analysis and understanding of PAI that offers relevant insights into foreign perceptions of the U.S. Students and researchers at the chosen institution would use AI to scan and analyze PAI on social media and other public platforms in support of this mission. This recommendation directly engages the AEN's second and third objectives while indirectly supporting the first and fourth. By engaging academic spaces, USCYBERCOM will be able to take advantage of the expertise and innovation that academia offers and increase talented researchers' awareness of the command, potentially strengthening USCYBERCOM's future ability to attract talent and perform this work itself.

Implementation

Relying on analysis of best practices and lessons learned through execution of initiatives similar to that proposed here, this section outlines a potential implementation plan for the above recommendation, reviews stakeholder involvement and roles, and anticipates challenges.

Identifying Partner Institutions

In order to implement this type of academic partnership as part of the AEN, USCYBERCOM will need to establish a contractual vehicle to support such an effort and identify a partner institution. As it looks for academic institutions with which to partner, USCYBERCOM can facilitate this process by consulting with other DoD entities, such as the Defense Advanced Research Projects Agency (DARPA) and its Information Innovation Office (IIO), to take advantage of their academic networks and knowledge of institutions specializing in relevant skills. The IIO, for example, focuses in part on exploring and advancing a full range of AI techniques. Contacts there may be aware of universities with skills in this area that have interest in military AI partnerships, or they may be able to help inform the search process in other ways (Defense Advanced Research Projects Agency, 2022).

As the AEN is a relatively young initiative and is still forming, USCYBERCOM may also look to recent agreements that it has already made with certain institutions. Where there has been commitment to cooperate, but specifics of agreements have not yet been solidified, USCYBERCOM may alter these agreements to incorporate the proposed program if possible. Before committing significant resources, USCYBERCOM may choose to evaluate possible partner institutions by collaborating on shorter term projects that demonstrate an institution's capacity to leverage AI in support of the command's mission.

Stakeholder Considerations

Once implemented, this initiative would involve stakeholders from across sectors: military, academia, and industry. Given this project's focus on AI, USCYBERCOM would likely need to involve personnel from both the J-2 and the J-9, which runs innovation for the entire Cyber Mission Force. While students and other researchers at academic facilities would be doing the majority of analytic work, supplying a facility with two to three USCYBERCOM officials would help maintain agency control and oversight over the process. Active USCYBERCOM presence would also promote the mutual awareness and human connection critical to advancing the program's key goals and fostering an environment that is beneficial to all participating stakeholders.

Anticipating Challenges

Differences in worldview, culture, and approaches to problem-solving among sectors, especially between military practitioners and those from academic backgrounds, may pose challenges. Academics often approach challenges as puzzles and opportunities for exploration. They typically seek out their subjects of interest, which can deter outreach across disciplines and fields. In contrast, military officials must meet the immediate needs of the moment (Mosser, 2010). This is especially the case for USCYBERCOM, which supports and enables the work of all Combatant Commands as

part of the Joint Force (Nakasone, 2020). Unfamiliarity with the military and the secretive nature of intelligence could also exacerbate perceived differences and make challenges more difficult to overcome.

In its efforts to overcome these differences, USCYBERCOM should prioritize communication, cooperation, and mutual understanding among stakeholders from different backgrounds. One way to do this is through collaborative design of the program process (Mosser, 2010), which would encourage development of mutual purpose and stakeholder buy-in. Doing so would also account for the nuances of the particular institution and enable the team to best take advantage of its unique technical strengths and other capabilities. This would encourage maximum effectiveness. Maintaining consistent visibility of USCYBERCOM officials in the workspace by stationing personnel there and through regular visits by high-ranking officials would also help foster a sense of shared interests and collaboration.

Best Practices

Analysis of similar programs, including the NSA's LAS at NC State University, and the perspectives of personnel involved in these programs underscores the need to incorporate several key principles in the implementation of the proposed program. Program elements that would strengthen and maintain a robust sense of collaboration between stakeholders include: a mutual sense of benefits from the work, mutual trust among personnel, common understanding of rules of engagement and communication processes that consider varied backgrounds, open access to each other, incentives, and a mutual sense of mission criticality (Shipman, 2017).

The proposed program offers a technical solution to the problem of interest in this report and related issues, including limited USCYBERCOM resources and personnel. Its execution would entail use of AI methods, researchers to apply these methods, and increased USCYBERCOM access to relevant analysis of PAI providing insight into foreign perception of the U.S. This insight can then be used in identification of potential partner countries. The technical nature of this program should produce measurable outcomes demonstrating whether it actually increases the amount of relevant PAI analysis that the command can access and the degree to which this analysis enhances USCYBERCOM understanding of foreign perception in support of Command goals.

To increase the likelihood of program success, USCYBERCOM officials and other stakeholders should work together to outline benchmarks for success at the beginning of this process and schedule multi-stakeholder check-ins to encourage accountability and measure progress. In order to manage risk, USCYBERCOM might consider a one-year trial period wherein these check-ins can be used to determine whether the program should continue, as well as opportunities for improvement. Formal reviews of LAS and similar existing initiatives demonstrate the utility of surveying program participants to gauge perceptions of success and challenges in the workplace in support of efforts to assess and optimize performance (Vogel & Tyler, 2019; Wilson et al., 2019).

If the program is determined to be sufficiently successful after this trial period, USCYBERCOM might consider investing more resources into the initiative and potential expansion to other institutions.

Conclusion

Amid rising aggression by adversaries in the cyber domain, USCYBERCOM has identified the need to leverage PAI in its efforts to better understand foreign perceptions of the U.S. and use this understanding to identify potential international partners. As USCYBERCOM works to confront this security environment with limited resources, answering this need will become increasingly essential to accomplishment of the command's mission objectives.

This report recommends that USCYBERCOM address this policy problem by initiating a partnership with an academic institution, where researchers can work alongside USCYBERCOM personnel to use AI processes in analysis of PAI and glean insight into foreign perception for USCYBERCOM decisionmakers. This effort would be incorporated as part of USCYBERCOM's AEN initiative.

Such a partnership is not just an opportunity to meet the challenge of the moment. Successful implementation of the proposed program will drive innovation, lay a foundation for further cross-sector collaboration, and offer key lessons and insights on best practices as USCYBERCOM continues to pursue that collaboration while extracting maximum value for the command.

Appendix

Figure 1

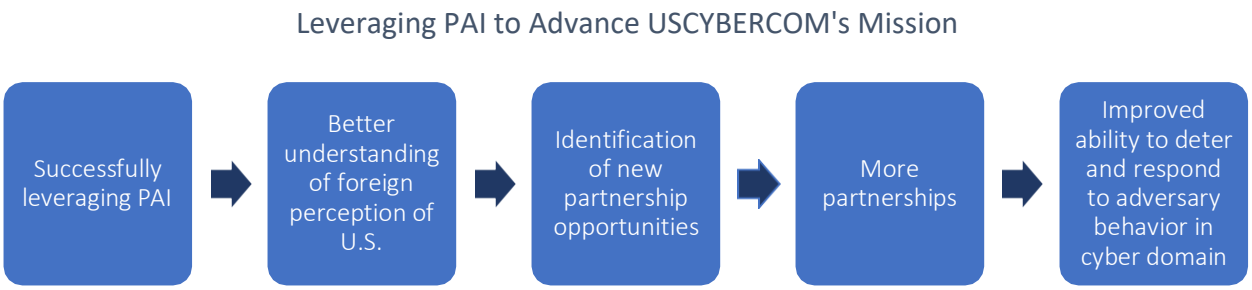
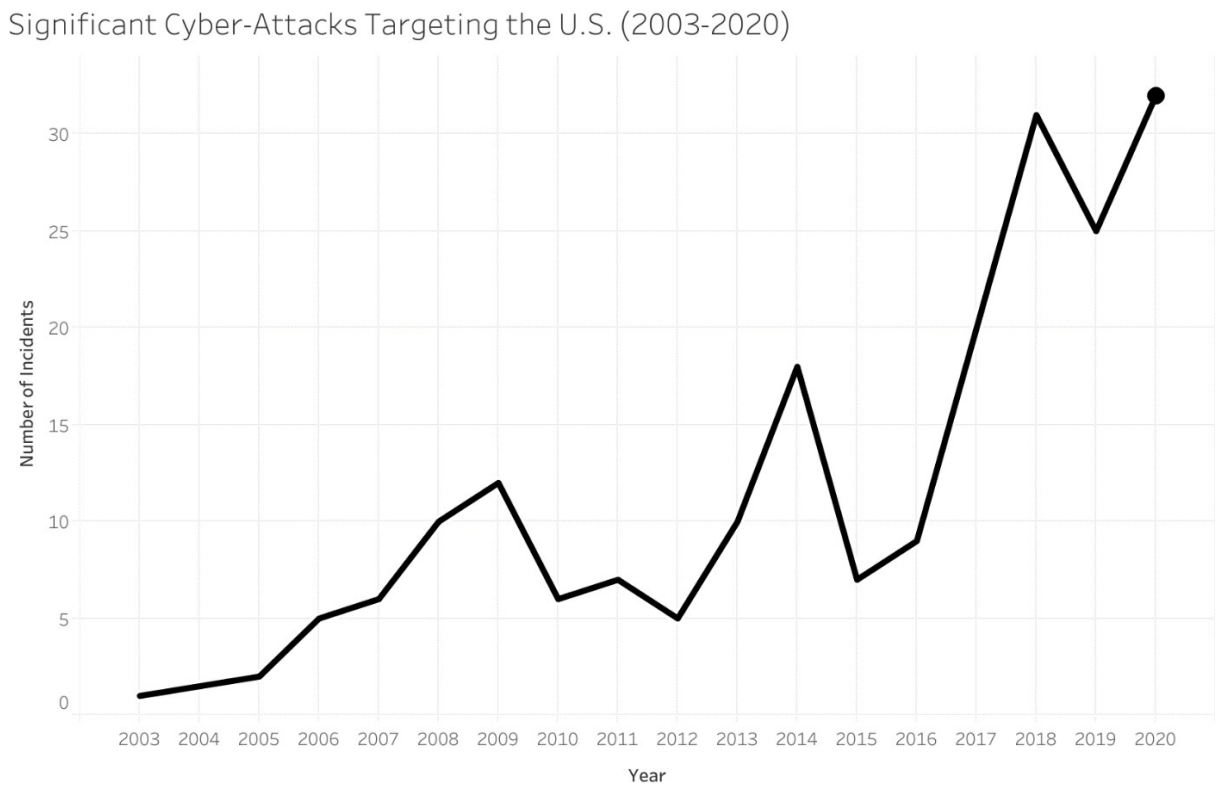


Figure 2



Graph shows trend over time in number of significant cyber-attacks targeting the U.S. between 2003 and 2020. "Significant cyber-attacks" are those targeting government agencies or defense and high-tech companies, as well as economic cybercrimes resulting in losses of over a million dollars. Data sourced from Center for Strategic & International Studies (2021).

Cost Evaluation for Alternative 1

Alternative 1 proposes interagency cooperation between USCYBERCOM and another federal agency. Cost for this alternative is estimated using CBO estimates for other federal interagency initiatives, which are overviewed below.

S. 1867, Department of Homeland Security Unmanned Aircraft Systems Coordinator Act (2019)

This bill would direct the Department of Homeland Security to appoint an official to coordinate department efforts to counter drone threats and provide that official with a staff. CBO cost calculations assume the coordinator would need roughly five senior employees to assist in coordinating efforts, which would include information-sharing with the private sector (Congressional Budget Office, 2019b).

Assuming the initiative would be implemented from 2019 through December 2022, CBO estimates S. 1867 would cost roughly $3 million in total.

S. 1294, Broadband Interagency Coordination Act of 2019

This bill would mandate an interagency agreement among the Federal Communication Commission, Department of Agriculture, and the National Telecommunications and Information Administration that coordinates federal funding distribution for deployment of broadband internet technologies. The initiative would entail data and information sharing among these agencies.

CBO estimates the cost of the initiative as roughly $1 million over five years (2019-2024) (Congressional Budget Office, 2019a).

S. 615, Trans-Sahara Counterterrorism Partnership Program Act of 2021

This bill seeks to codify the Trans-Sahara Counterterrorism Partnership, which is an initiative to coordinate federal efforts to combat violent extremism in North and West Africa. The Department of State would lead the effort in conjunction with the DoD and the U.S. Agency for International Development, and the bill would require the State Department to craft and execute an interagency strategy and to evaluate its progress along with a strategy for coordinating related development, diplomatic, and national security plans and objectives.

CBO estimates that the bill would cost $2 million over five years (2021-2026) (Congressional Budget Office, 2021a).

H.R. 1339, Advanced Air Mobility Coordination and Leadership Act (2021)

This bill would require the Department of Transportation to establish an interagency working group consisting of representatives from at least eight federal agencies. The initiative would evaluate and coordinate efforts related to advanced air mobility.

Assuming the bill would be implemented by the end of 2021, CBO estimates implementation would cost $1 million over a four-year period (2022-2026) (Congressional Budget Office, 2021b).

Cost Calculation

Alternative 1			
Bill	**Cost**	**Length of Implementation Period (Years)**	**Average Cost Per Year**
S. 1867	$ 3,000,000.00	3	$ 1,000,000.00
S. 1294	$ 1,000,000.00	5	$ 200,000.00
S. 615	$ 2,000,000.00	5	$ 400,000.00
H.R. 1339	$ 1,000,000.00	4	$ 250,000.00
			Average Annual Cost (All Programs)
			$ 462,500.00

Cost Evaluation for Alternative 3

Sample Cost Comparison sourced from DoD instructions initially published July 3, 2013 and revisited July 1, 2020 (Department of Defense, 2020, p. 32).

Type of Personnel	Base Pay with Locality and BAH	Programmed Amount	Full Cost to DoD	Full Cost to Government
Military O-5, 20 Years of Service	$137,164	$193,920	$209,009	$236,814
Civilian GS-14, Step 5	$119,238	$155,367	$164,570	$178,971
Contractor (government site)	N/A	$195,667	$195,667	$195,667
Contractor (contractor site)	N/A	$240,390	$240,390	$240,390

Cost estimate for Alternative 3 based on "Full Cost to DoD" value for "Civilian GS-14, Step 5". "Full Cost to DoD" for civilian personnel includes "Programmed Amount" and cost of recruitment and advertising, training, and child development.

Cost Evaluation for Alternative 4

In 2014, the cost of each individual program within the NSA's broader laboratory outreach efforts was estimated to be $1 million to $2.5 million (Rockwell, 2014). Using the Bureau of Labor Statistics' CPI Inflation calculator, a similar program in today's dollars is estimated to cost about $1.2 million to $3 million.

The DoD sample cost comparison used in Alternative 3 cost estimates was also used here to estimate the full cost of proposed civilian or military USCYBERCOM personnel oversight (Department of Defense, 2020). This cost was then added to the estimated cost of the program based on similar existing programs to reach the final cost estimate.

Bibliography

Ackerman, R. K. (2021, February 2). *Cyberthreat's Most Effective Attack Vector Is the Economy*. SIGNAL Magazine. https://www.afcea.org/content/cyberthreat%E2%80%99s-most-effective-attack-vector-economy

Afrobarometer. (2022). *Surveys and methods*. Afrobarometer. https://afrobarometer.org/surveys-and-methods

Air Force. (2022). *Publicly Available Information (PAI) Collection Management*. SBIR. https://www.sbir.gov/node/2101893

Ang, C. (2021, May 10). *The Most Significant Cyber Attacks from 2006-2020, by Country*. Visual Capitalist. https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

ATLAS. (2022). *About ATLAS*. Atlas Advisors. https://www.atlasadvisors.us/about.html

Booz Allen Hamilton. (2022). *Analytics and AI*. Booz Allen Hamilton. https://www.boozallen.com/expertise/analytics.html

Buarque, D. (2019). Brazil Is Not (Perceived as) a Serious Country: Exposing Gaps between the External Images and the International Ambitions of the Nation. *Brasiliana: Journal for Brazilian Studies*, *8*(1–2), 285–314. https://doi.org/10.25160/bjbs.v8i1-2.112957

Buhmann, A. (2016a). Towards an integrative model of the country image. In A. Buhmann (Ed.), *Measuring Country Image: Theory, Method, and Effects* (pp. 27–47). Springer Fachmedien. https://doi.org/10.1007/978-3-658-15407-3_2

Buhmann, A. (2016b, September 16). *Measuring Country Image: A New Model*. USC Center on Public Diplomacy. https://uscpublicdiplomacy.org/blog/measuring-country-image-new-model

Buhmann, A., & Ingenhoff, D. (2015). The 4D Model of the country image: An integrative approach from the perspective of communication management. *International Communication Gazette*, *77*(1), 102–124. https://doi.org/10.1177/1748048514556986

Burt, T. (2020, September 29). *Microsoft report shows increasing sophistication of cyber threats*. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Chapman, J. (2020, December 22). *How to use publicly available information to support enterprise security*. Security Magazine. https://www.securitymagazine.com/articles/93934-how-to-use-publicly-available-information-to-support-enterprise-security

Cobwebs Technologies. (2022, February 14). *Harnessing the Power of Publicly Available Information*. Cobwebs Webint Solutions. https://cobwebs.com/harnessing-the-power-of-publicly-available-information/

Congressional Budget Office. (2019a). *S. 1294, Broadband Interagency Coordination Act of 2019 | Congressional Budget Office*. Congressional Budget Office. https://www.cbo.gov/publication/55377

Congressional Budget Office. (2019b). *S. 1867, DHS Countering Unmanned Aircraft Systems Coordinator Act | Congressional Budget Office*. Congressional Budget Office. https://www.cbo.gov/publication/55469

Congressional Budget Office. (2021a). *S. 615, Trans-Sahara Counterterrorism Partnership Program Act of 2021 | Congressional Budget Office*. Congressional Budget Office. https://www.cbo.gov/publication/57102

Congressional Budget Office. (2021b). *H.R. 1339, Advanced Air Mobility Coordination and Leadership Act | Congressional Budget Office*. Congressional Budget Office. https://www.cbo.gov/publication/57477

Cordesman, A. H. (2021a, January 7). *Making America Great? Global Perceptions of China, Russia, and the United States: The International Scorecard*. Center for Strategic & International Studies.

https://www.csis.org/analysis/making-america-great-global-perceptions-china-russia-and-united-states-international

Cordesman, A. H. (2021b, June 14). *Strategic Competition and Foreign Perceptions of the United States*. Center for Strategic & International Studies. https://www.csis.org/analysis/strategic-competition-and-foreign-perceptions-united-states

Dalton, S. (1972). Foreign Student Perceptions of the United States. *Indiana Studies in Prediction*, *20*. https://eric.ed.gov/?id=ED068058

Defense Advanced Research Projects Agency. (2022). *Information Innovation Office (I2O)*. Defense Advanced Research Projects Agency. https://www.darpa.mil/about-us/offices/i2o?ppl=collapse

Defense Civilian Intelligence Personnel System. (n.d.). *Office of Personnel Management Estimated Salary Table DCIPS Compensation Administration*. https://dcips.defense.gov/Portals/50/Documents/Training_Docs/HR%20Elements%20for%20HR%20Practitioners/Participant%20Guide/PG_HR_Prac_Ch_6-Compensation_Admin_Dec15.pdf

Deloitte. (2022). *Analytics*. Deloitte Insights. http://www2.deloitte.com/us/en/insights/topics/analytics.html

Department of Defense. (2016). *DOD Manual 5240.01: Procedures Governing the Conduct of DOD Intelligence Activities*. https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887

Department of Defense. (2018). *Summary of the Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*. Department of Defense.

Department of Defense. (2020). *Estimating and Comparing the Full Costs of Civilian and Active Duty Military Manpower and Contract Support*. Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/704104p.pdf

Department of State. (2018). *Department of State Procurement Forecast Fiscal Year 2019 [Dataset]*. Department of State. https://www.state.gov/procurement-forecast

Department of State. (2021). *Department of State Procurement Forecast Fiscal Year 2022 [Dataset]*. Department of State. https://www.state.gov/procurement-forecast

Department of State. (2022). *About Us – Bureau of Intelligence and Research*. United States Department of State. https://www.state.gov/about-us-bureau-of-intelligence-and-research/

Director of National Intelligence—Open Source Center. (n.d.). Federation of American Scientists. Retrieved February 5, 2022, from https://irp.fas.org/dni/osc/index.html

Eftimiades, N. (2018, December 4). *The Impact of Chinese Espionage on the United States*. Diplomat. https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states/

Everwatch. (2022). *What We Do*. Everwatch. https://everwatchsolutions.com/what-we-do/

Gallup. (2014, October 14). *How Does the Gallup World Poll Work?* Gallup.Com. https://www.gallup.com/178667/gallup-world-poll-work.aspx

Go, F. M., & Govers, R. (2011). *International Place Branding Yearbook 2011*. Palgrave Macmillan UK.

Gupta, N., Sergi, B. J., Tran, E. D., Nek, R., & Howieson, S. V. (2014). *Research Collaborations Between Universities and Department of Defense Laboratories*. Institute for Defense Analyses.

Hysenagolli, G. (2019). *Request for Quotation (RFQ) SOL_72016520Q00001*. USAID. https://www.usaid.gov/sites/default/files/documents/1863/Request_for_Quotation_RFQ_Sol_720165-20-Q-00001_-_DG_Survey_2019.pdf

INTERPOL report shows alarming rate of cyberattacks during COVID-19. (2020, August 4). INTERPOL. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Johnson, D. B. (2022, January 7). *Cyber Command announces partnership with 84 universities*. SC Media. https://www.scmagazine.com/analysis/careers/cyber-command-announces-partnership-84-universities

Konkel, F. R. (2016, July 26). *CIA Director: Open Source a 'Tremendous Advantage.'* Nextgov.Com. https://www.nextgov.com/analytics-data/2016/07/cia-director-open-source-tremendous-advantage/130226/

Konkel, F. R. (2018, January 11). *Pentagon Thwarts 36 Million Email Breach Attempts Daily*. Nextgov.Com. https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/

Koré, Y. (2016). *Issuance of this solicitation does not in any way obligate the USG to award a contract not does it commit to pay for any incurred by the Offerer in the preparation and submission of a proposal. Award will be subject to funds availability following the proper completion of required USAID internal processes and other internal USAID approvals.* USAID. https://www.usaid.gov/sites/default/files/documents/1860/Signed%20RFP-SOL-625-16-000006%20(1).pdf

Landon-Murray, M., & Coulthart, S. (2020). Intelligence studies programs as US public policy: A survey of IC CAE grant recipients. *Intelligence and National Security*, *35*(2), 269–282. https://doi.org/10.1080/02684527.2019.1703487

Lane, J. (2021, June 2). *The 10 Most Spoken Languages In The World*. Babbel Magazine. https://www.babbel.com/en/magazine/the-10-most-spoken-languages-in-the-world

Leidos. (2022). *Company*. Leidos. https://www.leidos.com/company

Magu, S. M. (2013). *Soft Power Strategies in US Foreign Policy: Assessing the Impact of Citizen Diplomacy on Foreign States' Behavior* [Old Dominion University]. ODU Digital Commons. https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1075&context=gpis_etds

Mosser, M. W. (2010). Puzzles versus Problems: The Alleged Disconnect between Academics and Military Practitioners. *Perspectives on Politics*, *8*(4), 1077–1086.

Myauo, M. (2016). The U.S. Department of Defense Cyber Strategy: A Call to Action Partnership International Engagement on Cyber XI: Forum: The Role of Strategy in Securing a Nation in the Cyber Domain. *Georgetown Journal of International Affairs*, *17*(3), 21–29.

Nakasone, P. M. (2020). *Statement of General Paul M. Nakasone Commander United States Cyberspace Command Before House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities*. https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf

NC State University. (2022a). *Analytics—Laboratory for Analytic SciencesLaboratory for Analytic Sciences*. Laboratory for Analytic Sciences. https://ncsu-las.org/research-areas/predictive-analytics/

NC State University. (2022b). *Laboratory for Analytic Sciences*. Laboratory for Analytic Sciences. https://ncsu-las.org/

NC State University. (2022c). *Sensemaking—Laboratory for Analytic SciencesLaboratory for Analytic Sciences*. Laboratory for Analytic Sciences. https://ncsu-las.org/research-areas/sensemaking/

NC State University. (2022d). *Structured Analytic Tradecraft*. Laboratory for Analytic Sciences. https://ncsu-las.org/research-areas/structured-analytic-techniques/

Peraton. (2022). *Company—About*. Peraton. https://www.peraton.com/company/

Perlroth, N. (2021, July 19). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

Perrett, C. (2021, June 12). *Major cyberattacks have rocked the US, and there are "a lot of different ways that ransomware actors can disrupt everyone's lives," experts say*. Business Insider. https://www.businessinsider.com/cyberattacks-are-on-the-rise-in-the-us-experts-say-2021-6

Pew. (2022). *International Surveys*. Pew Research Center. https://www.pewresearch.org/our-methods/international-surveys/

Pomerleau, M. (2022, January 18). *US Cyber Command will use new academic engagement network to tackle cyber challenges*. C4ISRNet. https://www.c4isrnet.com/cyber/2022/01/18/new-academic-partnership-to-provide-military-access-to-more-cyber-research-on-hard-problems/

Ramakrishnan, N., Butler, P., Muthiah, S., Self, N., Khandpur, R. P., Saraf, P., Wang, W., Cadena, J., Vullikanti, A., Korkmaz, G., Kuhlman, C., Marathe, A., Zhao, L., Hua, T., Chen, F., Lu, C.-T., Huang, B., Srinivasan, A., Trinh, K., & Mares, D. (2014). "Beating the news" with EMBERS: Forecasting Civil Unrest using Open Source Indicators. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. https://doi.org/10.1145/2623330.2623373

Reibstein, D. J. (2016). *Billions in the Balance: Why Managing a Nation's Brand Matters*. Wharton.

Rockwell, M. (2014, May 7). *NSA funds "science of cybersecurity" research*. FCW. https://fcw.com/security/2014/05/nsa-funds-science-of-cybersecurity-research/254405/

SAIC. (2022). *Analytics*. SAIC. https://www.saic.com/what-we-do/mission-support/analytics-and-simulation

Sanger, D. E., Perlroth, N., & Schmitt, E. (2020, December 15). Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. *The New York Times*. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Schumacher, S., & Kent, N. (2020, April 2). *8 charts on internet use around the world as countries grapple with COVID-19*. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/

Scroxton, A. (2021, April 8). *Nation-state cyber attacks double in three years*. ComputerWeekly.Com. https://www.computerweekly.com/news/252499042/Nation-state-cyber-attacks-double-in-three-years

Significant Cyber Incidents | Center for Strategic and International Studies. (2021). Center for Strategic & International Studies. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Smith, A. (2021, January 1). *Text - H.R.6395 - 116th Congress (2019-2020): William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* (2019/2020) [Legislation]. Congress.Gov. https://www.congress.gov/bill/116th-congress/house-bill/6395/text

Sood, A. K., & Enbody, R. J. (2013). *Targeted Cyber Attacks—A Superset of Advanced Persistent Threats*. https://dokumen.tips/documents/targeted-cyber-attacks-a-superset-of-advanced-persistent-threats.html

Tau, B., & Volz, D. (2021, December 10). Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data. *Wall Street Journal*. https://www.wsj.com/articles/defense-intelligence-agency-expected-to-lead-militarys-use-of-open-source-data-11639142686

Tomczak, M. J., Torroll, M. N., & Kaloshi, M. B. (2021). Stewards of the Status Quo: US Air, Space, and Cyber Imperatives in the Indo-Pacific Gray Zone. *Journal of Indo-Pacific Affairs*. https://www.airuniversity.af.edu/JIPA/Display/Article/2743844/stewards-of-the-status-quo-us-air-space-and-cyber-imperatives-in-the-indo-pacif/#sdendnote22sym

U.S. Office of Personnel Management. (1958). *Position Classification Standard for International Cooperation Series, GS-0136*. U.S. Office of Personnel Management. https://www.opm.gov/policy-data-

oversight/classification-qualifications/classifying-general-schedule-positions/standards/0100/gs0136.pdf

Vogel, K. M., & Tyler, B. B. (2019). Interdisciplinary, cross-sector collaboration in the US Intelligence Community: Lessons learned from past and present efforts. *Intelligence and National Security*, *34*(6), 851–880.

Webb, D. (2021, November 9). *11/9 APP Check-In* [Personal communication].

Who We Are. (2017, April 3). ORB International. https://orb-international.com/about/

Wicker, M. (n.d.). *Explaining Publicly Available Information | Babel Blog*. Babel Street. Retrieved April 5, 2022, from https://www.babelstreet.com/blog/pai-explained

Wilson, A., Schmidt, M., Schmidt, L., & Winter, B. (2019). Immersive Collaboration on Data Science for Intelligence Analysis. *Harvard Data Science Review*, *1*(2). https://doi.org/10.1162/99608f92.4a9eef8d

World Population Clock: 7.9 Billion People (2022) - Worldometer. (2022). WorldOMeter. https://www.worldometers.info/world-population/