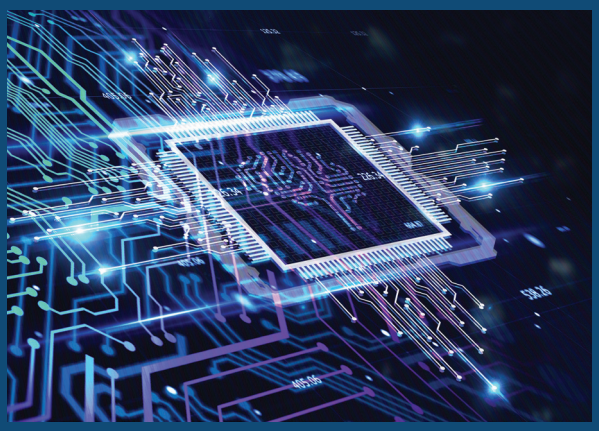
SELECT RAND RESEARCH ON THE

INFORMATION ENVIRONMENT

2014–2020



RAND CORPORATION

For more information on this publication, visit www.rand.org/t/CPA614-4.

Published by the RAND Corporation, Santa Monica, Calif.

Cover: greenbutterfly/Adobe Stock, putilov_denis/Adobe Stock, WrightStudio/Adobe Stock; Page iii: putilov_denis/Adobe Stock.

FOREWORD

This brief volume is an important resource for anyone who is interested in gaining an informed understanding of operations in the information environment. Large quantities of information are created and collected on a daily basis worldwide. As the information environment rapidly expands and evolves, we are challenged not only to exploit the power of information but also to manage unprecedented risks to individuals, institutions, and our nation.

For several decades after its inception in 1948, the RAND Corporation made many foundational contributions to the evolution of the Information Age, including contributions to digital computing, programming languages, modeling and simulation, information security, and the internet. Over the past two decades, RAND has focused its research on aspects of the information environment that relate to national security. These aspects include operations in the information environment and the staff integrating function of information operations; social media; data analytics and big data; intelligence collection and analysis; and information security, privacy, and information-sharing. This volume succinctly surveys the best recent examples from this ongoing body of research that are cleared for public release and synthesizes their collective results.

Readers of this volume will gain familiarity with current and emergent insights on what strategies and practices are likely to be most-effective at operating in and influencing across a dynamic information environment. Keeping abreast of the most advanced thinking is particularly important in this policy area because it remains highly dynamic, with many unsettled questions and contested issues.

RAND research has long helped to define and refine the way the Department of Defense and other U.S. departments and agencies think about operations in the information environment, but additional research is needed to support the full effective integration of information operations into strategy, planning, and processes. This volume might help to identify opportunities for additional analyses to fill in knowledge gaps, address emerging questions, or extend the scope of past research. We welcome your suggestions.

* * *

This volume is one of a series initiated by RAND Arroyo Center, the Army's federally funded research and development center for studies and analysis. Inaugural titles include Security Cooperation; Counterinsurgency, Stability Operations, Support to Foreign Internal Defense, Nation-Building, and Special Operations; China; and Information Operations, Information Warfare, and Influence. Each succinctly synthesizes decades of RAND research and analysis on topics that represent perennial and evolving challenges to our nation's security.

RAND conducted each of the analyses at the request of a senior leader, uniformed or civilian, who faced a major decision and required high-quality, objective research to help inform it. As a result, each analysis was designed to be not only rigorous and reliable but also responsive, relevant, and immediately useful.

These studies also display the variety of analytic capabilities, methods, and tools that RAND has applied—and sometimes originated or extended—to address our national security challenges. They illustrate the power of applied transdisciplinary research to address complex policy issues through engagement with stakeholders and continual adaptation to exploit improved data sources and advanced analytic methods. The studies highlighted and synthesized here were sponsored by the U.S. Army, the U.S. Air Force, and the Office of the Secretary of Defense and conducted in three federally funded research and development centers managed by RAND: RAND Arroyo Center, Project AIR FORCE, and the National Defense Research Institute.

Though intended to be timely, these analyses have retained their value over time. Together they provide a coherent accumulation of innovation, knowledge, and insights, and they demonstrate the value of sustained, strategic investments in defense analysis.

In short, they fulfill RAND's mission to improve policy and decisionmaking through research and analysis and exemplify its core values of quality and objectivity.

Sally Sleeper

Vice President, Army Research Division
Director, RAND Arroyo Center

Contents

TAKING STOCK OF RAND'S RESEARCH ABOUT THE INFORMATION ENVIRONMENT

Information, or how to obtain knowledge from investigation, study, or instruction,[1] has always been a critical and broad element of the human experience. However, the advent of the internet and the increasing connectivity of humanity has exponentially increased the pool of information and data available to us. This environment provides opportunities for and presents challenges to the United States; harnessing the power of information and using it to increase efficiencies, improve security, and deny access and advantages to adversaries are all topics that RAND Corporation research has examined in this sphere.

Both the *National Security Strategy of the United States of America* and *National Defense Strategy of the United States of America* recognize the information environment (IE) as central in warfare, although both documents emphasize the use of information in contexts short of open warfare or in the digital realm.[2] The U.S. Department of Defense (DoD) defines the *IE* as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[3] DoD operates explicitly in the IE and acknowledges that the inherent informational aspects of all military activities have effects in and throughout the IE. Public and private organizations also operate in this space, along with friendly and adversarial governments, nonstate actors, and private citizens. Moreover, the tools and capabilities in this realm are no longer the exclusive purview of national governments; the proliferation of information sources and analytic tools in the public realm has only increased the complexity of the IE for DoD. Since the end of the Cold War, the United States has expected dominance in its military endeavors, including those in the IE. In the resulting decades, China and Russia have been developing their capabilities to conduct operations in this realm against the United States and its allies. With a return to near-peer competition, DoD must consider these adversarial capabilities and how it will confront and mitigate them.[4]

RAND has a long history of researching the IE, but this compendium focuses on the past six years, because of the dynamic nature of the information ecosystem and the fast pace of technological change. The bulk of the works in this summary focus on DoD efforts in the IE, though a few studies have also looked at the activities of other agencies and departments, including the Department of State, the intelligence community (IC), and federal and municipal law enforcement elements. The large number of actors, programs, and activities touching the IE across departments and agencies presents several

[1] Merriam-Webster.com, "Information," webpage, undated.

[2] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018, p. 3; White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017, pp. 31–32.

[3] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington, D.C., January 2021, p. 104.

[4] Christopher M. Dougherty, *Why America Needs a New Way of War,* Washington, D.C.: Center for a New American Security, June 2019.

Abbreviations

C2	command and control	**ISIS**	Islamic State of Iraq and Syria
DoD	U.S. Department of Defense	**OIE**	operations in the information environment
IC	intelligence community	**OSINT**	Open Source Intelligence
IE	information environment		

challenges, including coordinating across multiple competing interests while also protecting the civil rights and privacy of U.S. citizens. Ultimately, the research grapples with how the United States can and should effectively leverage the IE to engage and defeat adversaries while protecting the national interest and the civil liberties of individual Americans.

As noted in the very definition of the word *information*, the term is broad and encompasses diverse actions, functions, and subjects. RAND's research appropriately covers the breadth and depth of the IE as it relates to the national security realm. For example, one effort to organize key types of information relevant for military operations identified six categories, which include situational awareness, command and control (C2), how to influence adversaries and how they influence military forces, and how information affects actors in the environment who are not direct adversaries.[5] This is just one example of an attempt to define information and bound it for a specific project. This summary does not use this taxonomy to organize RAND research on the IE, choosing instead to use broad categories according to the general focus of the research projects, which recognized the breadth of research projects on the IE.

The remainder of this introduction discusses the main findings from RAND research in five main areas. As it remains a dynamic and constantly evolving area of research, overlap exists among many of the sections. The first section addresses the literature on operations in the information environment (OIE) and the staff integrating function of information operations. Historical usage of the term *information operations* at times blurred the distinction between these two realms. Although the section notes differences between the two, it has addressed them together. The second section focuses on social media. The third broaches data analytics (formerly focusing on big data), while the fourth distills the findings from research on intelligence collection and analysis. The fifth section discusses RAND work on information security and privacy and information-sharing (although these are two notionally distinct areas of research, they are presented in a single section because many of the key issues overlap).

Operations in the Information Environment

DoD now uses OIE to describe a sequence of actions with the common purpose of affecting the perceptions, attitudes, and decisionmaking of relevant actors.[6] RAND's research in this space focuses on how DoD can improve its own OIE and the staff function that supports these operations, and also investigates adversarial efforts to shape the IE. At the core, analysis has addressed the key question: How does the United States effectively conduct OIE to maintain national security and defend against the operations of our adversaries?

One key insight that emerges is that **DoD has not effectively integrated the IE into operational planning, doctrine, or processes, instead considering traditional land, air, and sea operations separately from operations in the information space**. The authors of *Improving C2 and Situational Awareness for Operations in and Through the Information Environment* note that this is a critically important gap as our adversaries increasingly weaponize information.[7] *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment* (2018) reaffirms this assessment while adding that changes in the IE are because of technology proliferation among less sophisticated state and nonstate actors. This has expanded the threat environment, especially as these actors do not operate within the same legal and ethical constraints as the United States and its allies.[8] This gap is also

[5] Christopher Paul, Yuna Huh Wong, and Elizabeth M. Bartels, *Opportunities for Including the Information Environment in U.S. Marine Corps Wargames*, Santa Monica, Calif.: RAND Corporation, RR-2997-USMC, 2020.

[6] Christopher Paul, "Is It Time to Abandon the Term Information Operations," *Strategy Bridge,* March 13, 2019.

[7] Christopher Paul, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2489-OSD, 2018.

[8] Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018.

reflected in the lack of consistent inclusion of the IE into DoD wargaming efforts. Wargames provide opportunities for operators and support staff to plan and practice responses in a conflict. Therefore, these games must reflect the realities of warfare, in particular against the "increasingly important information-based tools of warfare," as noted in *Opportunities for Including the Information Environment in U.S. Marine Corps Wargames* (2020).[9] Raising the IE to the level of land, air, and sea operations will only further enhance U.S. national security efforts, recognizing that the effects of OIE extend beyond the IE.[10]

With external experts and Congress also arguing that the decentralized nature of DoD information efforts across the services harms U.S. efforts against our adversaries,[11] RAND research has also focused on how to overcome coordination issues within DoD and how to assess and evaluate operations conducted in the IE. *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness* (2015) focused on psychological operations in Afghanistan and documented a disconnect between the doctrine relating to conducting operations in the IE and the implementation of that doctrine in the field. The report recommends that DoD develop a holistic strategy to communicate with local populations via key community influencers and to understand the needs and interests of the target population.[12] To support the practitioner, RAND developed evaluation toolkits and handbooks to provide recommendations on how to apply doctrine to the battlespace. However, evaluation of influence efforts is not always straightforward. **It can be difficult to measure changes in audience behavior and attitudes, and it can take a great deal of time for DoD's inform, influence, and persuade efforts to have an effect**, as *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference* (2015) explains.[13] Assessment is made easier when objectives are clear and specific and when assessment design is part of planning. *Frameworks for Assessing USEUCOM Efforts to Inform, Influence, and Persuade* (2020) reaffirms these findings, while also noting that when assessments are systematically developed and executed, appropriate allocation of resources, refinement of plans, and realization of objectives are more likely to occur.[14]

In contrast with some of DoD's struggles to develop a coherent IE strategy and approach, U.S. adversaries are significantly more advanced at least in the strategic planning for such activities. *Hostile Social Manipulation: Present Realities and Emerging Trends* (2019) notes that adversaries **employ targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage to the target state**. The authors argue for establishing a framework for understanding the scope and consequences of hostile social manipulation.[15] This type of manipulation can lead to *virtual societal warfare*. Set in the digital realm, this type of warfare "involves efforts to manipulate or disrupt the information foundations of the effective functioning of economic and social systems." As warfare continues to expand in the IE, advanced democracies, including the United States, must enhance resilience against information-based social manipulation and understand the vulnerabilities

[9] Paul, Wong, and Bartels, 2020.

[10] Paul, Wong, and Bartels, 2020.

[11] Mark Pomerleau, "Congress Wants to Up DoD's Game in the Information Environment," *C4ISRNet,* December 10, 2019; Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Examination," *War on the Rocks*, June 14, 2019.

[12] Arturo Muñoz and Erin Dick, *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness*, Santa Monica, Calif.: RAND Corporation, PE-128-OSD, 2015.

[13] Christopher Paul, Jessica Yeats, Colin P. Clarke, and Miriam Matthews, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*, Santa Monica, Calif.: RAND Corporation, RR-809/1-OSD, 2015.

[14] Miriam Matthews, Christopher Paul, David Schulker, and David Stebbins, *Frameworks for Assessing USEUCOM Efforts to Inform, Influence, and Persuade*, Santa Monica, Calif.: RAND Corporation, RR-2998-EUCOM, 2020.

[15] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, Santa Monica, Calif.: RAND Corporation, RR-2713-OSD, 2019.

present in emerging technologies.[16] David Ronfeldt and John Arquilla (2020) emphasize these findings in an update to a 1999 RAND report discussing how to adapt U.S. strategy to the information age. In *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft*, they argue the decisive factor in war will increasingly be connected to "whose story wins" in the global commons; many adversaries have already developed and deployed weaponized narratives, strategic deception, and epistemic attacks to gain leverage in the IE.[17]

Social Media

RAND's work on social media related to national security generally falls into to two broad categories: (1) ways that DoD and law enforcement could leverage social media for their advantage, and (2) adversaries' usage of social media against the United States and U.S. partners and allies. Questions relating to social media collection and analysis, along with developing methods to leverage it in operations in the IE, remain critical and outstanding. DoD and federal, state, and local law enforcement must also consider how to protect the civil liberties of U.S. citizens when analyzing social media and while conducting operations that use those sources.

Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations (2017) begins with the following observation: **Social media analysis is playing an important and increasing role in advertising and academic research, but it also has significant potential to support military operations in the IE by providing a window into the perspectives, thoughts, and communications of a wide variety of relevant audiences**.[18] The report notes that existing legal and policy frameworks have not kept pace with the global expansion and reach of modern communication systems, which include the massive amounts of information produced by social media users on an hourly basis. In addition to providing recommendations for the most-effective analytic approaches for DoD to leverage social media analysis in operations in the IE, the authors provided a framework to consider legal, ethical, policy, technological, and training factors. In 2019's *Using Social Media and Social Network Analysis in Law Enforcement*, a panel of experts grappled with similar issues, but from the perspective of state and municipal law enforcement rather than national security. Stakeholders wanted to understand how to leverage social media in social network analysis but emphasized legal processes, providing transparency while ensuring privacy, and equitable justice as their primary concerns.[19]

In addition to adapting policy and legal frameworks to the new IE, research was undertaken to identify not only individuals participating in broad malign or subversive information efforts, but the whole structure supporting the operation. The authors of *Detecting Malign or Subversive Information Efforts over Social Media: Scalable Analytics for Early Warning* (2020) highlight **the "credibility gap" the United States has in detecting and addressing these malign campaigns in the public sphere**. Using a Russian case study, they adapted "an existing social media analysis method, combining network analysis and text analysis to map, visualize, and understand the communities interacting on social media." The analytic method required both machine-based approaches and human expertise to detect the misinformation campaign, and the authors recommended that the U.S. government not only implement the proof of concept but also develop

[16] Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2714-OSD, 2019.

[17] David Ronfeldt and John Arquilla, *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft*, Santa Monica, Calif.: RAND Corporation, PE-A237-1, 2020.

[18] William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, Santa Monica, Calif.: RAND Corporation, RR-1742-OSD, 2017.

[19] John S. Hollywood, Michael J. D. Vermeer, Dulani Woods, Sean E. Goodison, and Brian A. Jackson, *Using Social Media and Social Network Analysis in Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-2301-NIJ, 2018.

professional expertise to support early detection of such efforts.[20]

The importance of social media and its analysis holds not only for DoD and other U.S. agencies and departments but also for U.S. adversaries. RAND research on adversary use of social media has thus far predominantly focused on Russia, capturing a snapshot of its tactics and operations at the time of the project, as its capabilities continue to mature and evolve. RAND researchers have termed Russian activities in the IE as, "the firehose of falsehood," which has "two . . . distinctive features: high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions," which confuses and overwhelms its audience, according to *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (2016).[21] Unfortunately, this study also found that people are poor at discriminating truth from falsehood and, therefore, are more vulnerable to being manipulated than most realize.[22] Russian information efforts are not interested in emphasizing truth or being a credible source but rather aim to obfuscate facts and confuse their targets, and their contemporary methodology was noticed during and researched after the 2016 U.S. presidential election. Following the IC's public announcement of the Russian influence campaign, RAND researchers provided recommendations about how to combat Russian disinformation in *Countering Russian Social Media Influence* (2018). The authors note that Russian disinformation campaigns through social media are directed by senior levels of the Russian government and aim to **push several conflicting narratives simultaneously, deepening existing divisions within American society, and degrading trust in Western institutions and the democratic process.[23]** Additional RAND reports have documented similar Russian efforts against U.S. partner nations or countries where they perceive growing U.S. influence, such as Eastern Europe and Turkey.[24] In each of these situations, Russia seeks to exploit divisions and sow doubt in the relationship between the United States and these allies by leveraging the public information sphere on social media.

Foreign governments are not the only adversaries the United States must confront in the IE. Nonstate actors, such as al Qaeda and the Islamic State of Iraq and Syria (ISIS) took the media tools presented to them and revolutionized their usage to spread their message, recruit followers, and disrupt U.S. and coalition efforts to eliminate the threat from the terrorist group. In two projects, Elizabeth Bodine-Baron and Todd Helmus investigated ISIS' use of Twitter and identified ways to effectively counteract the group's messaging. In *Examining ISIS Support and Opposition Networks on Twitter* (2016), they identified opportunities to effectively undermine ISIS' Twitter effort by learning how ISIS supporters and their opponents leveraged Twitter.[25] In 2017, they investigated further ISIS' methods to empower opponents on Twitter, recommending that any Twitter campaign be supported by a larger effort to undermine ISIS messaging, working with influential local Twitter users, and

---

[20] William Marcellino, Krystyna Marcinek, Stephanie Pezard, and Miriam Matthews, *Detecting Malign or Subversive Information Efforts over Social Media: Scalable Analytics for Early Warning*, Santa Monica, Calif.: RAND Corporation, RR-4192-EUCOM, 2020.

[21] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016.

[22] The Stanford Internet Observatory notes how Russia, in particular, is leveraging this human weakness through narrative laundering operations. This technique represents a process of introducing state-developed narratives into the global commons via aligned publications (think tanks and media outlets), "useful idiots," and potentially witting contributors. For more information, see Renee Diresta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, Stanford, Calif.: Stanford Internet Observatory Cyber Policy Center, November 2019.

[23] Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018.

[24] Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018; Katherine Costello, *Russia's Use of Media and Information Operations in Turkey: Implications for the United States*, Santa Monica, Calif.: RAND Corporation, PE-278-A, 2018.

[25] Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, Calif.: RAND Corporation, RR-1328-RC, 2016.

tailoring messages to specific communities.[26] The IE short of war provides the United States and its adversaries multiple opportunities to achieve strategic policy goals.

Data Analytics

As mentioned in the previous section, civilians not associated with governments produce massive quantities of data on a daily basis. However, governments also regularly produce large amounts of data, whether in the public or private spheres. Considering the rise of attacks by state and nonstate hackers to gain primarily personally identifiable information, such as the hack against the U.S. Office of Personnel Management in 2015,[27] an opportunity exists to understand how and why adversaries might attempt to gain access to the same public data troves that DoD wishes to understand and those sensitive ones produced by the U.S. government. RAND research generally focused on how DoD can better assess the data it already possesses, especially in areas where the services are overwhelmed with collecting and producing mission-critical data. **However, opportunities remain to research adversarial efforts and priorities to gain access to sensitive U.S. data or the same public data to uncover and exploit U.S. vulnerabilities, which exist beyond leveraging publicly available social media information**.

Multiple reports focused on leveraging openly available data-driven research tools and mechanisms, such as Google Trends or Google AdWords, to better understand potential recruits' search methodologies or improve online outreach to those people. In 2016's *Searching for Information Online: Using Big Data to Identify the Concerns of Potential Army Recruits*, the authors argue that the anonymous data from those Google tools provide leading and lagging indicators about the evolution of a searcher's interest in a military career.[28] Research conducted through focus groups in 2019 revealed recruiting specialists recognized the potential privacy issues that could arise through this type of data mining, and sought to understand potential restrictions and constraints that exist in today's online world.[29]

In addition to recruiting, DoD recognizes that efficiencies can be gained by leveraging, organizing, and protecting data in the acquisition field. Over a period of five years and three separate projects, RAND researchers documented **that the process for gaining access to data is inefficient and might not provide access to the best data to support analysis**, according to *Issues with Access to Acquisition Data and Information in the Department of Defense* (2015).[30] Data remain critical to management and oversight of the acquisition process, but service cultures often have incompatible storage systems, privacy and security concerns, and limited methods to conduct analysis given these constraints.[31] *Issues with Access to Acquisition Data and Information in the Department of Defense: Doing Data Right in Weapon System Acquisition* (2017) found that large businesses also have these concerns and issues. Recommended best practices from the private sector included embracing a master data management system, which would formalize governance, improve the quality of structured and

[26] Todd C. Helmus and Elizabeth Bodine-Baron, *Empowering ISIS Opponents on Twitter*, Santa Monica, Calif.: RAND Corporation, PE-227-RC, 2017.

[27] Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," *Wired*, October 23, 2016.

[28] Salar Jahedi, Jennie W. Wenger, and Douglas Yeung, *Searching for Information Online: Using Big Data to Identify the Concerns of Potential Army Recruits*, Santa Monica, Calif.: RAND Corporation, RR-1197-A, 2016.

[29] Nelson Lim, Bruce R. Orvis, and Kimberly Curry Hall, *Leveraging Big Data Analytics to Improve Military Recruiting*, Santa Monica, Calif.: RAND Corporation, RR-2621-OSD, 2019.

[30] Jessie Riposo, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar, and Jerry M. Sollinger, *Issues with Access to Acquisition Data and Information in the Department of Defense*, Santa Monica, Calif.: RAND Corporation, RR-880/1-OSD, 2015.

[31] Philip S. Anton, Megan McKernan, Ken Munson, James G. Kallimani, Alexis Levedahl, Irv Blickstein, Jeffrey A. Drezner, and Sydne Newberry, *Assessing Department of Defense Use of Data Analytics and Enabling Data Management to Improve Acquisition Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-3136-OSD, 2019.

unstructured data and its ability to be analyzed, and encourage training programs.[32] Additional research considered storage methods and the feasibility of cloud computing for the voluminous amounts of data produced by the U.S. military.[33]

Intelligence Collection and Analysis

The expanding IE challenges the IC like few other U.S. government departments and agencies; not only does it have to manage the information it collects through clandestine and technical methods but it continues to struggle with incorporating the open source data (e.g., social media, press, big data) produced by the broader population. RAND researchers worked to identify ways the IC could manage multiple large data sources and incorporate publicly available information, technologies, and methods into their suite of capabilities while maintaining operational security. The 2017 *National Security Strategy of the United States* describes the environment the IC faces:

> America's ability to identify and respond to geostrategic and regional shifts and their political, economic, military, and security implications requires that the U.S. Intelligence Community (IC) gather, analyze, discern, and operationalize information. In this information-dominant era, the IC must continuously pursue strategic intelligence to anticipate geostrategic shifts, as well as shorter-term intelligence so that the United States can respond to the actions and provocations of rivals.[34]

Open Source Intelligence (OSINT) complements strategic and crisis intelligence analysis and production but is often underutilized because of **the difficulty in understanding emerging OSINT sources and methods, particularly social media platforms**.[35] RAND research suggests that, although commercial off-the-shelf tools are useful, it is likely they will have to be adapted for intelligence analysis purposes. Still, the rapid advances in machine learning and natural language processing likely will support analysis of open source data for intelligence purposes. It would behoove the IC to spend time investigating which tools and open data sources can be leveraged in the future. *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency* (2016) recommended that the agency look into efforts to recruit, train, and retain its own internal data science capabilities, taking advantage of the growing community and applying it to military intelligence analysis.[36] **However, commercial technologies affect how the public and private spheres interact, which is changing the way we conduct business, diplomacy, intelligence operations, and war and how we think about privacy, security, and secrecy**, which will continue to have ramifications on the legal frameworks that govern the IC and its analysis and collection capabilities, as highlighted in *A Rapidly Changing Urban Environment: How Commercial Technologies Can Affect Military Intelligence Operations* (2016).[37]

RAND has also continued to focus on traditional aspects of intelligence analysis, unrelated to the

---

[32] Megan McKernan, Nancy Young Moore, Kathryn Connor, Mary E. Chenoweth, Jeffrey A. Drezner, James Dryden, Clifford A. Grammich, Judith D. Mele, Walter T. Nelson, Rebeca Orrie, Douglas Shontz, and Anita Szafran, *Issues with Access to Acquisition Data and Information in the Department of Defense: Doing Data Right in Weapon System Acquisition*, Santa Monica, Calif.: RAND Corporation, RR-1534-OSD, 2017.

[33] Isaac R. Porche III, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman, *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information*, Santa Monica, Calif.: RAND Corporation, RR-315-NAVY, 2014; Kathryn Connor, Ian P. Cook, Isaac R. Porche III, and Daniel Gonzales, *Cost Considerations in Cloud Computing*, Santa Monica, Calif.: RAND Corporation, PE-113-A, 2014.

[34] White House, 2017, p. 31.

[35] Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Santa Monica, Calif.: RAND Corporation, RR-1964-OSD, 2018.

[36] Bradley Knopp, Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson, *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, RR-1582-DIA, 2016.

[37] William Young and David Stebbins, *A Rapidly Changing Urban Environment: How Commercial Technologies Can Affect Military Intelligence Operations*, Santa Monica, Calif.: PE-181-OSD, 2016.

issues of OSINT and data analytics. Understanding how to best train and prepare analysts for their roles within the national security community and how effective analytic capabilities are at providing effective recommendations remain of utmost importance to decisionmakers. *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis* (2016) describes an environment where intelligence analysts must be ready to support commanders across the entire spectrum of warfare, from irregular and terrorist threats to conventional war with a near-peer competitor. Although some processes, such as strong critical thinking and analysis skills and building collaborative networks, are needed regardless of the type of mission, the research uncovered challenges relating to the pace of future operations and the volume of information collected. Researchers recommended a renewed focus on training and developing analysts and the tools they have available to them.[38]

Information Security, Information-Sharing, and Privacy

With more data—and more touchpoints between individuals, corporations, and governments and the digital world—come more and greater risks that this information will be improperly protected or shared. Issues of privacy and security are embedded in all RAND work on information in a national security context. Questions about who owns data and how they control access to this information, the ability to analyze data, and how to guarantee the security of the data and its connections to the source (whether human- or systems-generated) are the key elements of concern moving forward as the world becomes more reliant on information systems. The European Union, DoD, National Institutes of Justice, and elements of the United Kingdom's regulatory community requested RAND's assistance in understanding the regulatory and legal frameworks currently available to protect individuals' privacy and information security across the spectrum of smartphones, the connectivity through the Internet of Things, and data breaches. **Education of consumers, policymakers, law enforcement, and private industry remains critical to ensure the protection of citizen's civil rights and the massive quantities of data collected.** Proliferation of technologies and further technological advances in those technologies will only increase the challenges presented to each of these groups. Therefore, an opportunity exists to conduct research on the policy and legal protections of the data and its producers.

RAND's research into the legal and regulatory ecosystem confronts the tension between technology and privacy. Looking into smartphones, researchers discovered that although **privacy-preserving technology is improving, it does not fully address users' privacy concerns, providing a space for policy regulation**, according to *Can Smartphones and Privacy Coexist?: Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices* (2016).[39] Cell phones are not the only technology concerning policymakers and consumers. Smart speakers, such as Amazon's Alexa, Apple's HomePod, and Google Assistant, are also under scrutiny. These tools consume and produce massive quantities of data, collecting personal information that raises critical security concerns for individuals, companies, policymakers, and even criminals who seek to leverage the tool.[40]

Law enforcement agencies must be especially concerned as they navigate the legal space between investigations to maintain order and the protection of individuals. Technology increases the ability to share information quickly among all levels of local,

[38] Brien Alkire, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Danescu, William Fry, D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie Riposo, Timothy Smith, and Alexander Stephenson, *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, Santa Monica, Calif.: RAND Corporation, RR-1330-AF, 2016.

[39] Arkady Yerukhimovich, Rebecca Balebako, Anne Boustead, Robert K. Cunningham, William Welser IV, Richard Housley, Richard Shay, Chad Spensky, Karlyn D. Stanley, Jeffrey Stewart, Ari Trachtenberg, and Zev Winkelman, *Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices*, Santa Monica, Calif.: RAND Corporation, RR-1393-DARPA, 2016.

[40] Neil Robinson, Jon Freeman, Jan Gaspers, Veronika Horvath, Tess Hellgren, and Alex Hull, *Living Room Connected Devices: Opportunities, Security Challenges and Privacy Implications for Users and Industry*, Santa Monica, Calif.: RAND Corporation, RR-604-OFCOM, 2014.

state, and federal agencies, but **limitations exist regarding information-sharing technology and policy**.[41] *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?* (2015) provides recommendations to federal, state, and local law enforcement agencies about how to navigate the numerous records management systems to protect information and still provide mechanisms to share with other law enforcement agencies when appropriate. Moreover, in some domestic security arenas, such as those related to transnational terrorism, the involvement of intelligence agencies can lead to civil liberty and privacy concerns. Popular sentiment supports the notion that information-sharing between these communities is critical, but analysts must remain vigilant as they adhere to legal constraints and as policymakers consider the effectiveness of sharing the information. Two separate projects led by Brian A. Jackson highlight that establishing methods to measure the effects of information-sharing between law enforcement agencies is necessary; *How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts* (2014) looked at improving methodologies for assessing outcome measures.[42] In *Knowing More, but Accomplishing What? Developing Approaches to Measure the Effects of Information-Sharing on Criminal Justice Outcomes* (2017), researchers found that for the system evaluated, significant correlations were discovered between the benefits of information-sharing and outcomes across the law enforcement enterprise.[43] Information-sharing implications also exist between the U.S. government and commercial enterprises[44] along with inside the U.S. federal interagency,[45] with proprietary data and privacy concerns at the top of the list.

The remainder of this document provides summaries of RAND's research in the aforementioned areas in greater detail. Projects are organized in reverse chronological order, following a basic format of the title of the document, the authors, document number and year, along with a link to the project's public webpage. In some instances, a project falls into more than one category. As a result, these projects were listed in multiple categories.

---

[41] John S. Hollywood and Zev Winkelman, *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?*, Santa Monica, Calif.: RAND Corporation, RR-645-NIJ, 2015.

[42] Brian A. Jackson, *How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts*, Santa Monica, Calif.: RAND Corporation, RR-380-OSD, 2014.

[43] Brian A. Jackson, Lane F. Burgette, Caroline Stevens, Claude Messan Setodji, Erinn Herberman, Stephanie Ann Kovalchik, Katie Mugg, Meagan Cahill, Jessica Hwang, and Joshua Lawrence Traub, *Knowing More, but Accomplishing What? Developing Approaches to Measure the Effects of Information-Sharing on Criminal Justice Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-2099-NIJ, 2017.

[44] David A. Galvan, Brett Hemenway, William Welser IV, and Dave Baiocchi, *Satellite Anomalies: Benefits of a Centralized Anomaly Database and Methods for Securely Sharing Information Among Satellite Operators*, Santa Monica, Calif.: RAND Corporation, RR-560-DARPA, 2014; Brett Hemenway, William Welser IV, and Dave Baiocchi, *Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing*, Santa Monica, Calif.: RAND Corporation, RR-344-AF, 2014.

[45] Daniel Gonzales, Sarah Harting, Jason Mastbaum, and Carolyn Wong, *Improving Interagency Information Sharing Using Technology Demonstrations: The Legal Basis for Using New Sensor Technologies for Counterdrug Operations Along the U.S. Border*, Santa Monica, Calif.: RAND Corporation, RR-551-OSD, 2014.

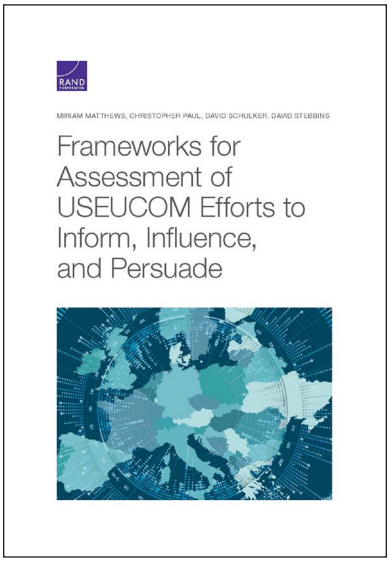
Annotated Bibliography

OPERATIONS IN THE INFORMATION ENVIRONMENT

Frameworks for Assessment of USEUCOM Efforts to Inform, Influence, and Persuade

Miriam Matthews, Christopher Paul, David Schulker, and David Stebbins

RR-2998-EUCOM (2020)



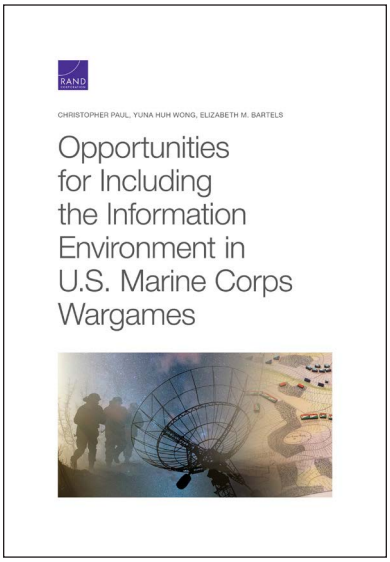
Campaigns to inform, influence, and persuade a range of foreign audiences are critical to achieving key U.S. national security objectives, but it can be challenging to assess the progress, performance, and effectiveness of these efforts in a real-world context. Systematically planned and implemented assessments are important in ensuring that finite resources are allocated appropriately, that plans can be refined, and that key objectives are realized. This report offers guidance, frameworks, and recommendations that can support and enhance assessment design and planning. Although they focus on U.S. European Command activities, they are instructive for any organization involved in planning and evaluating information campaigns.

Find the full report at www.rand.org/pubs/research_reports/RR2998

Opportunities for Including the Information Environment in U.S. Marine Corps Wargames

Christopher Paul, Yuna Huh Wong, and Elizabeth M. Bartels

RR-2997-USMC (2020)



The U.S. Marine Corps and joint concepts and thinking increasingly emphasize the role of information in military operations—from maintaining situational awareness to influencing adversary decisionmaking and understanding the behaviors of noncombatant populations. At the same time, wargaming is enjoying renewed prominence in the defense community as a tool to explore potential future conflicts and shape strategy. However, the information environment (IE) remains underdeveloped and underrepresented in wargames, both in the Marine Corps and across the U.S. Department of Defense. An examination of requirements, principles from military theory, current doctrine, and commercial gaming practices points to solutions and changes to game mechanics to better incorporate information considerations into wargame planning, development, and play in ways that can be customized according to available resources, capabilities, and goals. Recommendations target wargame sponsors, wargame designers, and those who are responsible for procuring new tools and recruiting personnel to support wargaming. Operations in the IE play a role across the spectrum of conflict, and their

effects and consequences extend beyond the IE. As the nature of conflict changes, it is critical that wargames reflect realities on the ground, supporting forces in using and defending against increasingly important information-based tools of warfare.

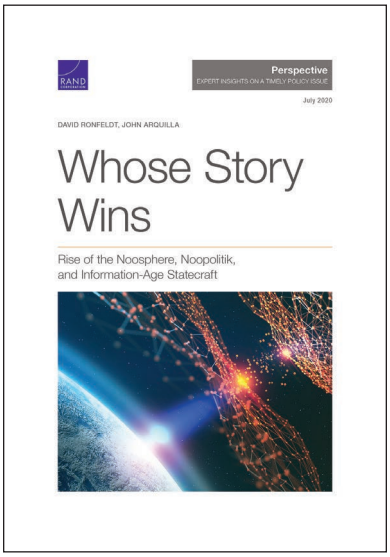
Find the full report at www.rand.org/pubs/research_reports/RR2997

Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft

David Ronfeldt and John Arquilla

PE-A237-1 (2020)

In this Perspective, the authors urge strategists to consider a new concept for adapting U.S. grand strategy to the information age—*noopolitik*, which favors the use of soft power—as a successor to realpolitik, with its emphasis on hard power. The authors illuminate how U.S. adversaries are already deploying dark forms of noopolitik—e.g., weaponized narratives, strategic deception, epistemic attacks. The authors propose new ways to fight back and discuss how the future of noopolitik might depend on what happens to the *global commons*—i.e., the parts of the Earth and space that fall outside national jurisdictions and to which all nations are supposed to have access. The authors expand on many of the ideas they first proposed in a 1999 RAND Corporation report titled *The Emergence of Noopolitik: Toward an American Information Strategy*, in which they describe the emergence of a new globe-circling realm: the noosphere. The authors explain that Earth first developed a *geosphere*, a geological mantle, and then a *biosphere*, consisting of plant and animal life. Third to develop will be the *noosphere*, a global thinking circuit and realm of the mind—a collective form of intelligence enabled by the digital information revolution. As the noosphere expands, it will profoundly affect statecraft; the conditions favoring traditional realpolitik strategies will erode, and the prospects for noopolitik strategies will grow. Thus, the decisive factor in today's and tomorrow's wars of ideas is bound to be whose story wins—the essence of noopolitik. To improve prospects for the noosphere and noopolitik, U.S. policy and strategy should, among other initiatives, treat the global commons as a pivotal issue area, uphold guarded openness as a guiding principle, and institute a requirement for periodic reviews of America's information posture.



Find the full document at www.rand.org/pubs/perspectives/PEA237-1

Hostile Social Manipulation: Present Realities and Emerging Trends

Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden

RR-2713-OSD (2019)

The role of information warfare in global strategic competition has become much more apparent in recent years. Today's practitioners of what this report's authors term hostile social manipulation employ targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage to the target state. These

emerging tools and techniques represent a potentially significant threat to U.S. and allied national interests. This report represents an effort to better define and understand the challenge by focusing on the activities of the two leading authors of such techniques—Russia and China. The authors conduct a detailed assessment of available evidence of Russian and Chinese social manipulation efforts, the doctrines and strategies behind such efforts, and evidence of their potential effectiveness. RAND analysts reviewed English-, Russian-, and Chinese-language sources; examined national security strategies and policies and military doctrines; surveyed existing public-source evidence of Russian and Chinese activities; and assessed multiple categories of evidence of effectiveness of Russian activities in Europe, including public opinion data, evidence on the trends in support of political parties and movements sympathetic to Russia, and data from national defense policies. The authors found a growing commitment to tools of social manipulation by leading U.S. competitors. The findings in this report are sufficient to suggest that the U.S. government should take several immediate steps, including developing a more formal and concrete framework for understanding the issue and funding additional research to understand the scope of the challenge.

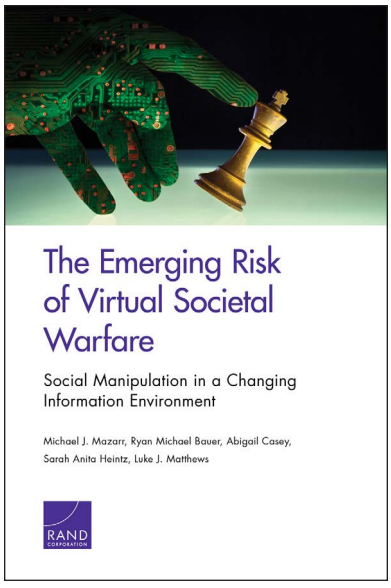
Find the full report at www.rand.org/pubs/research_reports/RR2713

The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment

Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews

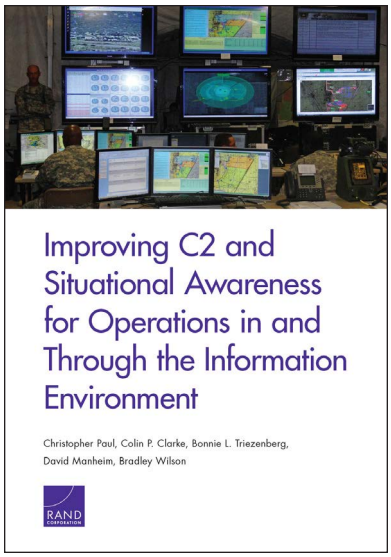
RR-2714-OSD (2019)

The evolution of advanced information environments is rapidly creating a new category of possible cyberaggression that involves efforts to manipulate or disrupt the information foundations of the effective functioning of economic and social systems. RAND researchers are calling this growing threat virtual societal warfare in an analysis of its characteristics and implications for the future. To understand the risk of virtual societal warfare, the authors surveyed evidence in a range of categories to sketch out some initial contours of how these techniques might evolve in the future. They grounded the assessment in (1) detailed research on trends in the changing character of the information environment in the United States and other advanced democracies; (2) the insights of social science research on attitudes and beliefs; and (3) developments in relevant emerging technologies that bear on the practices of hostile social manipulation and its more elaborate and dangerous cousin, virtual societal warfare. The authors then provide three scenarios for how social manipulation could affect advanced societies over the next decade. The analysis suggests an initial set of characteristics that can help define the emerging challenge of virtual societal warfare, including that national security will increasingly rely on a resilient information environment and a strong social topography, and that conflict will increasingly be waged between and among networks. Although more research is urgently required, the authors conclude by pointing to several initial avenues of response to enhance democratic resilience in the face of this growing risk, including by building forms of inoculation and resilience against the worst forms of information-based social manipulation and by better understanding the workings and vulnerabilities of emerging technologies.



Find the full report at www.rand.org/pubs/research_reports/RR2714

Improving C2 and Situational Awareness for Operations in and Through the Information Environment



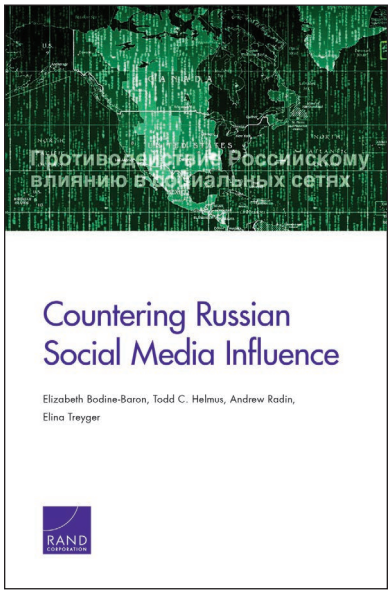
Christopher Paul, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson

RR-2489-OSD (2018)

The information environment (IE) is not a physical place and has not been defined as a warfighting domain in U.S. military doctrine. Targets of operations in and through the IE include human perceptions or behaviors: Weapons are ideas, and defenses are norms, beliefs, and traditions. Adding to the complexity of achieving command and control (C2) and situational awareness of the IE is the fact that the U.S. Department of Defense (DoD) has not effectively integrated the IE into operational planning, doctrine, or processes, instead considering traditional land, air, and sea operations separately from operations in the information space. However, every military activity has inherent informational aspects, and adversaries are increasingly using propaganda, misinformation, and other means to influence public perceptions, alliances, and decisions. Drawing on a review of doctrine and processes, the history of information operations and information-related capabilities, and interviews with subject-matter experts and stakeholders, this report presents a three-tiered vision for the role of information in U.S. military operations. It also identifies requirements for achieving effective C2 and situational awareness of the IE and presents a detailed analysis of seven ways to organize for this objective. Ultimately, addressing the gaps and shortfalls identified in this report will require a much stronger understanding of the IE, associated concepts and capabilities, and roles and responsibilities across the joint force.

Find the full report at www.rand.org/pubs/research_reports/RR2489

Countering Russian Social Media Influence



Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger

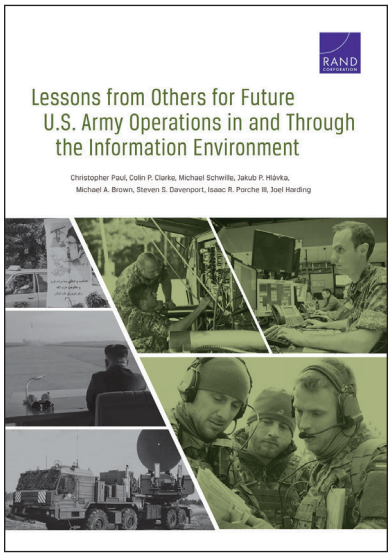
RR-2740-RC (2018)

In January 2017, the U.S. intelligence community released a public report detailing a Russian influence campaign, ordered by Russian President Vladimir Putin, to disrupt the U.S. presidential election. Part of a larger multifaceted approach, this campaign included social media–based disinformation spread by both automated bots and paid trolls. Russia's strategy was to push several conflicting narratives simultaneously, deepening existing divisions within American society and degrading trust in Western institutions and the democratic process. Although it is unknown what impact the campaign might have had on the 2016 presidential election, or on individual opinions, it is clear that Russia's efforts reached many Americans through a variety of social media platforms, including Twitter and Facebook. The Russian "disinformation chain" that directs these campaigns starts from the very top—from Russian leadership, to Russian organs and proxies, through amplification channels, such as social media platforms, and finally to U.S. media consumers. This report categorizes and analyzes different approaches and policy options to respond to the specific threat of Russian influence via disinformation spread on social media in the

United States. It is meant to educate and inform U.S. government officials considering policies for combating Russian disinformation; social media companies undertaking efforts to reduce the spread of disinformation on their platforms; non-governmental organizations, think tanks, and academics developing new approaches to address the threat of disinformation; and the American public.

Find the full report at www.rand.org/pubs/research_reports/RR2740

Lessons from Others for Future U.S. Army Operations in and Through the Information Environment



Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven S. Davenport, Isaac R. Porche III, and Joel Harding

RR-1925/1-A (2018)

Harnessing the power of old and new technology, it is easier than ever for U.S. allies and adversaries to reach—and influence—vast and varied audiences to achieve their strategic goals. Modern conflicts are fought as much in the information environment as on the physical battlefield, and the line between these domains is dissolving. Less sophisticated state actors and even nonstate actors have acquired capabilities previously available only to the most advanced nations to use information power in support of their objectives. Adversaries of the United States and its allies do not operate under the same legal and ethical constraints and are free to engage in offensive cyberwarfare, disseminate propaganda, censor traditional and online media, and threaten their detractors. As it prioritizes investments in future capabilities, the U.S. Army stands to benefit from an examination of the evolution of allied and adversary information campaigns, as well as their successes, failures, and potential future directions. This comparative analysis of 12 case studies highlights the capability areas in which others excel to guide the Army in either adopting or countering these principles and practices. A companion volume, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case Studies*, supports this comparative analysis with detailed assessments of the information-related activities and strategic goals of a range of allies, adversaries, and potential adversaries.

Find the full report at www.rand.org/pubs/research_reports/RR1925z1

Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case Studies

Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven S. Davenport, Isaac R. Porche III, and Joel Harding

RR-1925/2-A (2018)

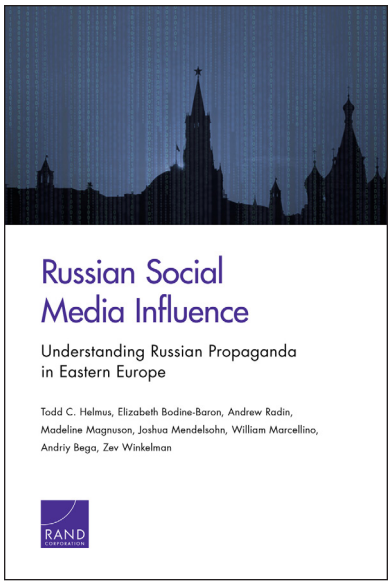
The companion collection to an earlier report (RR-1925/1-A) details 12 case studies. The report reviews the information-related activities and strategic goals of a range of allies, adversaries, and potential adversaries, highlighting insights for future U.S. Army force planning. This volume presents a comparative analysis of the cases, highlighting the capability areas in which others excel to guide the Army in either adopting or countering these practices and principles.

Find the full report at www.rand.org/pubs/research_reports/RR1925z2

Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe

Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman

RR-2237-OSD (2018)



A RAND Corporation study examined Russian-language content on social media and the broader propaganda threat posed to the region of former Soviet states that include Estonia, Latvia, Lithuania, Ukraine, and, to a lesser extent, Moldova and Belarus. In addition to employing a state-funded multilingual television network, operating various Kremlin-supporting news websites, and working through several constellations of Russia-backed "civil society" organizations, Russia employs a sophisticated social media campaign that includes news tweets, nonattributed comments on webpages, troll and bot social media accounts, and fake hashtag and Twitter campaigns. Nowhere is this threat more tangible than in Ukraine, which has been an active propaganda battleground since the 2014 Ukrainian revolution. Other countries in the region look at Russia's actions and annexation of Crimea and recognize the need to pay careful attention to Russia's propaganda campaign. To conduct this study, RAND researchers employed a mixed-methods approach that used careful quantitative analysis of social media data to understand the scope of Russian social media campaigns combined with interviews with regional experts and U.S. and North Atlantic Treaty Organization security experts to understand the critical ingredients to countering this campaign.

Find the full report at www.rand.org/pubs/research_reports/RR2237

Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe (Testimony Presented Before the Senate Select Committee on Intelligence)

Todd C. Helmus

CT-496 (2018)

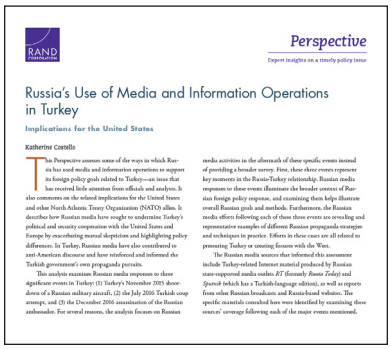
Todd Helmus shares lessons learned from a RAND study (RR-2237-OSD) in congressional testimony. Helmus provides an overview of Russian propaganda activities, reviews efforts to identify Russian propaganda on Twitter, and examines challenges confronting U.S. and European policymakers in the region. He concludes with recommendations for countering the Russian propaganda threat.

Find the full document at www.rand.org/pubs/testimonies/CT496

Russia's Use of Media and Information Operations in Turkey: Implications for the United States

Katherine Costello

PE-278-A (2018)



Russian media have sought to undermine Turkey's political and security cooperation with the United States and Europe by exacerbating mutual skepticism and highlighting policy differences. In Turkey, Russian media

have also contributed to anti-American discourse and have reinforced and informed the Turkish government's own propaganda pursuits. This analysis assesses how Russia has used media and information operations to pursue its foreign policy goals related to Turkey. It examines Russian media responses to three significant events in Turkey: (1) Turkey's November 2015 shootdown of a Russian military aircraft, (2) the July 2016 Turkish coup attempt, and (3) the December 2016 assassination of the Russian ambassador. Russian media efforts following these events exemplify the propaganda strategies of amplification of genuine uncertainty, creation of opportunistic fabrications, and use of multiple contradictory narratives. These strategies have supported Russian foreign policy objectives, which include undermining the North Atlantic Treaty Organization (NATO) and fomenting mutual suspicion between Turkey and its Western allies; enlisting Ankara's support and impeding its opposition to Russian actions in Eurasia and the Middle East; and influencing Turkish internal political developments to make Turkey a more compliant partner. The U.S. government, NATO, and independent media watch groups should take steps to monitor Russian media efforts in Turkey and outside coverage of Turkey. In addition, the U.S. government, other governments, and media watch groups should continue to monitor Turkish government efforts to stifle independent media in the country and to create a propaganda arm that might emulate well-honed Russian practices.

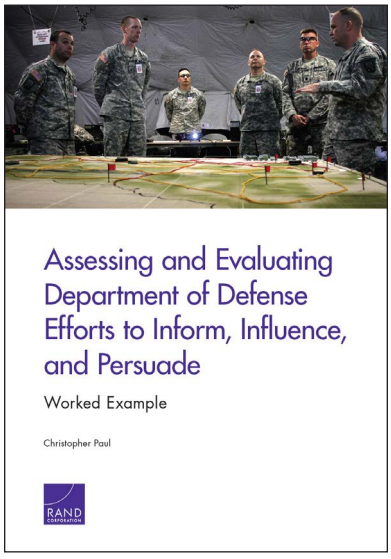
Find the full document at www.rand.org/pubs/perspectives/PE278

Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Worked Example

Christopher Paul

RR-809/4-OSD (2018)

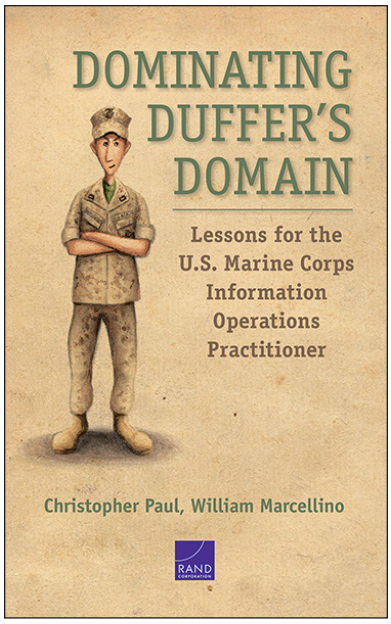
To achieve key national security objectives, the U.S. government and the U.S. Department of Defense (DoD) must communicate effectively and credibly with a broad range of foreign audiences. DoD spends more than $250 million per year on inform, influence, and persuade (IIP) efforts. It is clearly important to measure the performance and effectiveness of these efforts, but assessment has remained a challenge for DoD. To better support IIP planners and assessment practitioners, this report presents a realistic but fictional scenario as context for a step-by-step example of how assessment planning should work in practice. In the process, it demonstrates several core principles of effective assessment articulated in previous RAND research, along with insights and best practices for developing assessments that can accurately measure progress toward campaign objectives and directly support decisionmaking.



Accompanying volumes include, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference* (a quick-reference guide to the best practices presented here for personnel responsible for planning, executing, and assessing DoD IIP efforts), *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: An Annotated Reading List* (a self-study reading list in best assessment practices across a range of sectors), and *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners* (an easy-to-navigate, quick-reference guide to planning and conducting assessments of DoD IIP efforts, analyzing the data generated, and presenting the results).

Find the full report at www.rand.org/pubs/research_reports/RR809z4

Dominating Duffer's Domain: Lessons for the U.S. Marine Corps Information Operations Practitioner



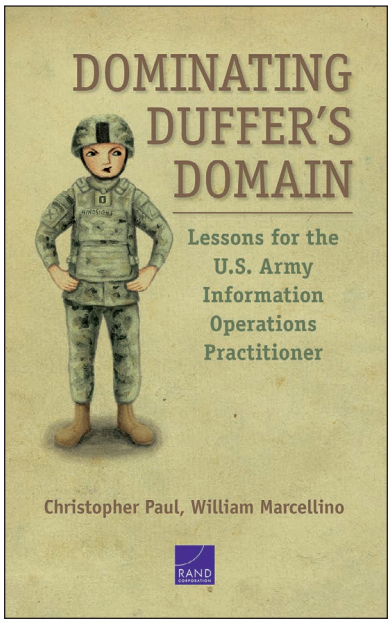
Christopher Paul and William Marcellino

RR-1166-1-OSD (2017)

More than a century after its release, *The Defence of Duffer's Drift*, by Major General Sir Ernest Swinton, has become an enduring military classic. This piece of instructional fiction, in which the narrator learns from his operational mistakes over a series of dreams, has earned a place in military classrooms and has inspired military leaders, analysts, and historians. Indeed, the narrative form can be a powerful teaching and learning tool. To support the U.S. Marine Corps and its curriculum for information operations personnel, RAND has adapted the premise of General Swinton's work for a modern-day audience and a different problem set. The fictitious narrator, Captain I. N. Hindsight, takes readers repeatedly through the same mission over the course of six dreams in which he makes shortsighted decisions, critical miscalculations, and smaller mistakes that contribute to spectacular failures until his accumulated lessons ultimately allow him and the command he supports to succeed. The fabricated instructional scenario draws on actual historical operations, alternative directions that these operations could have taken, and realistic challenges that a Marine Corps information operations planner might face. The 26 concise lessons in this volume offer insight that, ideally, the practitioner will not need to acquire through hindsight.

Find the full report at www.rand.org/pubs/research_reports/RR1166-1

Dominating Duffer's Domain: Lessons for the U.S. Army Information Operations Practitioner



Christopher Paul and William Marcellino

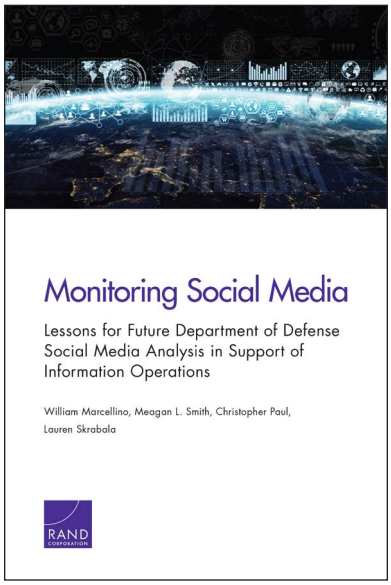
RR-1166/1-A (2017)

More than a century after its release, *The Defence of Duffer's Drift*, by Major General Sir Ernest Swinton, has become an enduring military classic. This piece of instructional fiction, in which the narrator learns from his operational mistakes over a series of dreams, has earned a place in military classrooms and has inspired military leaders, analysts, and historians. Indeed, the narrative form can be a powerful teaching and learning tool. To support the U.S. Marine Corps and its curriculum for information operations personnel and U.S. Army efforts to better integrate information operations into operational planning, RAND has adapted the premise of General Swinton's work for a modern-day audience and a different problem set. The fictitious narrator, Captain I. N. Hindsight, takes readers repeatedly through the same mission over the course of six dreams, making shortsighted decisions, critical miscalculations, and smaller mistakes that contribute to spectacular failures until accumulated lessons ultimately allow him and the command he supports to succeed. The fabricated instructional scenario draws on actual historical operations, alternative directions that these operations could have taken, and realistic challenges that a Marine Corps or

an Army information operations planner might face. The 26 concise lessons in this volume offer insight that, ideally, the practitioner will not need to acquire through hindsight.

Find the full report at www.rand.org/pubs/research_reports/RR1166z1

Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations



William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala

RR-1742-OSD (2017)

Social media analysis is playing an important and increasing role in advertising and academic research, but it also has significant potential to support military information operations by providing a window into the perspectives, thoughts, and communications of a wide range of relevant audiences. Although there are compelling national security reasons to field a social media analysis capability, the U.S. Department of Defense (DoD) must do so while navigating U.S. law and cultural norms and under conditions of great uncertainty. Existing legal and policy frameworks have not anticipated the rapid pace and global reach of modern communication networks, and questions of cost and implementation hinder the development of a robust social media analysis capability and the most fruitful applications for these analyses. To support DoD's assessment of the benefits, trade-offs, and implementation challenges that it will face as it expands its capacity for social media analysis, this report reviews the analytic approaches that will be most valuable for information operations, as well as legal, ethical, policy, technological, and training considerations. It also includes a set of recommendations to help DoD navigate this terrain while building a robust, effective social media analysis capability to support operations worldwide.

Find the full report at www.rand.org/pubs/research_reports/RR1742

The Weaponization of Information: The Need for Cognitive Security (Testimony Presented Before the Senate Armed Services Committee, Subcommittee on Cybersecurity)

Rand Waltzman

CT-473 (2017)

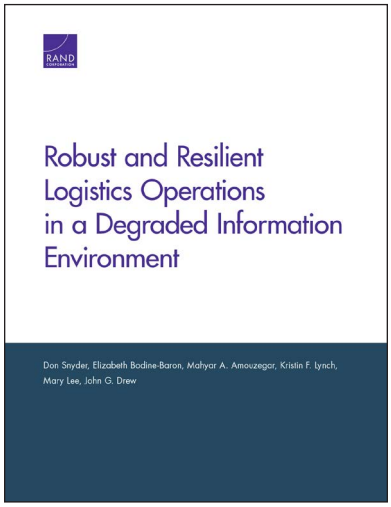
Today, thanks to the internet and social media, the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality. That manipulation is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with. Today, many actors are exploiting these vulnerabilities. The situation is complicated by the increasingly rapid evolution of technology for producing and disseminating information. For example, over the past year, we have seen a shift from the dominance of text and pictures in social media to recorded video, and even recorded video is being superseded by live video. As the technology evolves, so do the vulnerabilities. At the same time, the cost of the technology is steadily dropping, which allows more actors to enter the scene. In this testimony, Rand Waltzman discusses the threat of information operations in general and in the Russian context specifically, and recommends the creation of a Center for Cognitive Security to defend in the information environment.

Find the full document at www.rand.org/pubs/testimonies/CT473

Robust and Resilient Logistics Operations in a Degraded Information Environment

Don Snyder, Elizabeth Bodine-Baron, Mahyar A. Amouzegar, Kristin F. Lynch, Mary Lee, and John G. Drew

RR-2015-AF (2017)



Logistics operations depend on accurate information. Even relatively small errors in support systems can, in some circumstances, have large effects on operations. But errors are inevitable, so logistics operations should be robust to errors, whether they are a random occurrence or the result of a deliberate, targeted cyberattack. The U.S. Air Force asked RAND Project AIR FORCE to determine where it is most fruitful to focus effort in making changes to tactics, techniques, and procedures to improve an airman's ability to detect, evaluate, and mitigate significant corruption of logistics data. The goal is to respond to errors in data before they have a significant negative effect on combat operations. Recommendations include defining, within logistics policy, what measures the logistics community should take in response to each information operations condition level and creating a new central body (perhaps within an existing organization)—the Global Data Integrity Cell—that would receive all reports of suspected data anomalies to enable enterprise-wide situational awareness.

Find the full report at www.rand.org/pubs/research_reports/RR2015

The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It

Christopher Paul and Miriam Matthews

PE-198-OSD (2016)

In this Perspective, the authors characterize the contemporary Russian model for propaganda as "the firehose of falsehood" because of two of its distinctive features: high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions. In the words of one observer, "[N]ew Russian propaganda entertains, confuses and overwhelms the audience."

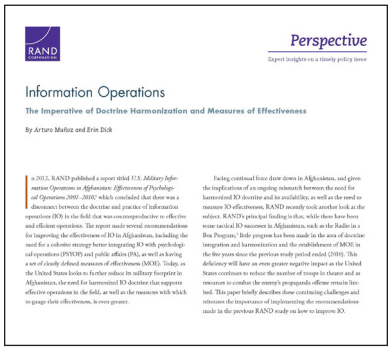
Contemporary Russian propaganda has at least two other distinctive features. It is rapid, continuous, and repetitive, and it lacks commitment to consistency. Interestingly, several of these features run directly counter to the conventional wisdom on effective influence and communication from government or defense sources, which traditionally emphasize the importance of truth, credibility, and the avoidance of contradiction. Despite ignoring these traditional principles, Russia seems to have enjoyed some success under its contemporary propaganda model, either through more direct persuasion and influence or by engaging in obfuscation, confusion, and the disruption or diminution of truthful reporting and messaging. The authors offer several possible explanations for the effectiveness of Russia's firehose of falsehood. Our observations draw from a concise, but not exhaustive, review of the literature on influence and persuasion, as well as experimental research from the field of psychology. They explore the four identified features of the Russian propaganda model and show how and under what circumstances each might contribute to effectiveness. Many successful aspects of Russian propaganda have surprising foundations in the psychology literature, so the authors conclude with a brief discussion of possible approaches from the same field for responding to or competing with such an approach.

Find the full document at www.rand.org/pubs/perspectives/PE198

Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness

Arturo Muñoz and Erin Dick

PE-128-OSD (2015)


RAND

Perspective

Expert insights on a timely policy issue

Information Operations

The Imperative of Doctrine Harmonization and Measures of Effectiveness

By Arturo Muñoz and Erin Dick

In an update to a 2012 RAND report on information operations (IO) in Afghanistan, this Perspective describes the continuing challenges of IO doctrine integration and harmonization and the establishment of measures of effectiveness for IO within the Department of Defense. Despite recommendations made in the 2012 report, little progress has been made in these areas, which will have an even greater negative impact as the United States reduces the number of troops in theater and as resources to combat the enemy's propaganda offense remain limited.

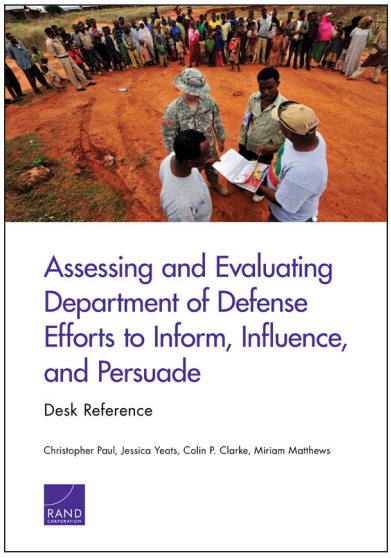
Find the full document at www.rand.org/pubs/perspectives/PE128

Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference

Christopher Paul, Jessica Yeats, Colin P. Clarke, and Miriam Matthews

RR-809/1-OSD (2015)

To achieve key national security objectives, the U.S. government and the U.S. Department of Defense (DoD) must communicate effectively and credibly with a broad range of foreign audiences. DoD spends more than $250 million per year on inform, influence, and persuade (IIP) efforts, but how effective (and cost-effective) are they? How well do they support military objectives? Could some of them be improved? If so, how? It can be difficult to measure changes in audience behavior and attitudes, and it can take a great deal of time for DoD IIP efforts to have an impact. DoD has struggled with assessing the progress and effectiveness of its IIP efforts and in presenting the results of these assessments to stakeholders and decisionmakers. To address these challenges, a RAND study compiled examples of strong assessment practices across sectors, including defense, marketing, public relations, and academia, distilling and synthesizing insights and advice for the assessment of DoD IIP efforts and programs. These insights and attendant best practices will be useful to personnel who plan and assess DoD IIP efforts and those who make decisions based on assessments, particularly those in DoD and Congress who are responsible for setting national defense priorities and allocating the necessary resources. In addition to identifying where and why efforts have been successful, assessment can help detect imminent program failure early on, saving precious time and resources. An accompanying volume, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners*, offers a quick-reference guide to the best practices presented here for personnel responsible for planning, executing, and assessing DoD IIP efforts.



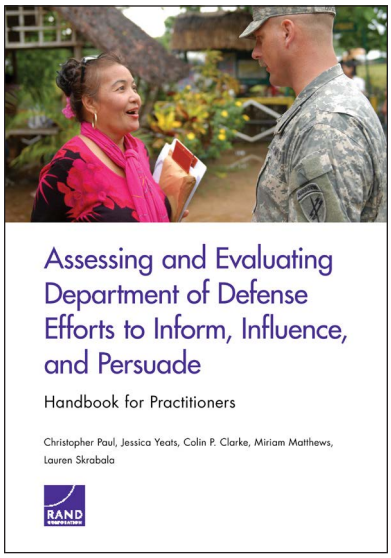
Find the full report at www.rand.org/pubs/research_reports/RR809z1

Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners

Christopher Paul, Jessica Yeats, Colin P. Clarke, Miriam Matthews, and Lauren Skrabala

RR-809/2-OSD (2015)

To achieve key national security objectives, the U.S. government and the U.S. Department of Defense (DoD) must communicate effectively and credibly with a broad range of foreign audiences. DoD spends more than $250 million per year on inform, influence, and persuade (IIP) efforts, but how effective (and cost-effective) are they? How well do they support military objectives? Could some of them be improved? If so, how? DoD has struggled with assessing the progress and effectiveness of its IIP efforts and in presenting the results of these assessments to stakeholders and decisionmakers. To address these challenges, a RAND study compiled examples of strong assessment practices across sectors, including defense, marketing, public relations, and academia, distilling and synthesizing insights and advice for the assessment of DoD IIP efforts and programs. This handbook was designed to be an easy-to-navigate, quick-reference guide to planning and conducting assessments of DoD IIP efforts, analyzing the data generated, and presenting the results. It also offers some background on current assessment practices in DoD and the typical users and uses of DoD IIP assessment results. A companion volume, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*, offers a more detailed exploration and additional examples of assessment in practice.



Find the full report at www.rand.org/pubs/research_reports/RR809z2

Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: An Annotated Reading List

Christopher Paul, Jessica Yeats, Colin P. Clarke, and Miriam Matthews

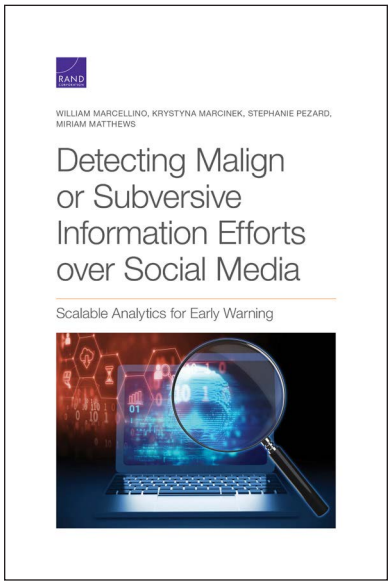
RR-809/3-OSD (2015)

The U.S. Department of Defense (DoD) has struggled to assess the progress and effectiveness of its efforts to inform, influence, and persuade audiences in support of key national security objectives. One reason is that it lacks personnel with sufficient expertise in assessment and evaluation. Although the department is making an effort to infuse sound assessment principles in doctrine and to expand assessment-related course offerings in the military-academic sector, these efforts will take time to bear fruit. These temporary shortfalls extend to the evaluation and assessment of DoD efforts to inform, influence, and persuade. To help fill the gap, RAND produced a reading list for self-study in best assessment practices across a range of sectors. The reading list has two purposes: to provide resources for new assessment personnel to cement and broaden their assessment and evaluation expertise and to serve as a general list of resources that can be made available to assessment stakeholders to improve their assessment expertise. It supplements two companion volumes, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference* and *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners*.

Find the full report at www.rand.org/pubs/research_reports/RR809z3

SOCIAL MEDIA

Detecting Malign or Subversive Information Efforts over Social Media: Scalable Analytics for Early Warning



William Marcellino, Krystyna Marcinek, Stephanie Pezard, and Miriam Matthews

RR-4192-EUCOM (2020)

The United States has a capability gap in detecting malign or subversive information campaigns before these campaigns substantially influence the attitudes and behaviors of large audiences. Although there is ongoing research into detecting parts of such campaigns (e.g., compromised accounts and "fake news" stories), this report addresses a novel method to detect whole efforts. The authors adapted an existing social media analysis method, combining network analysis and text analysis to map, visualize, and understand the communities interacting on social media. As a case study, they examined whether Russia and its agents might have used Russia's hosting of the 2018 World Cup as a launching point for malign and subversive information efforts. The authors analyzed approximately 69 million tweets in three languages about the World Cup in the month before and the month after the event, and they identified what appear to be two distinct Russian information efforts, one aimed at Russian-speaking and one at French-speaking audiences. Notably, the latter specifically targeted the populist *gilets jaunes* (yellow vests) movement; detecting this effort months before it made headlines illustrates the value of this method. To help others use and develop the method, the authors detail the specifics of their analysis and share lessons learned. Outside entities should be able to replicate the analysis in new contexts with new data sets. Given the importance of detecting malign information efforts on social media, it is hoped that the U.S. government can efficiently and quickly implement this or a similar method.

Find the full report at www.rand.org/pubs/research_reports/RR4192

Social Media and the Army: Implications for Outreach and Recruiting

Jennie W. Wenger, Heather Krull, Elizabeth Bodine-Baron, Eric V. Larson, Joshua Mendelsohn, Tepring Piquado, and Christine Anne Vaughan

RR-2686-A (2019)

As the U.S. population has increasingly adopted social media platforms, the U.S. Army has established its own recruiting website and social media accounts to facilitate communication and interaction with potential recruits, family members, and friends. While the growth in social media use has expanded the options available for Army recruiting, it also raises questions as to how the Army can best leverage technology to improve the effectiveness of its recruiting and the ways it connects with youth. The Army Marketing and Research Group (AMRG) asked RAND Arroyo Center to examine these issues and to develop strategies and recommendations. Given the advances in the use of technology, the goal in this report is to analyze several online and social media platforms used by the Army, in particular GoArmy.com (the Army's main recruiting and outreach webpage) and the Facebook and Twitter accounts maintained by AMRG. The authors focus on these three platforms because they are used by AMRG as its primary means of communication and outreach. They

analyze various measures to understand whether and how potential recruits and others are engaging with these platforms. They also present information about the likely outcomes of the Army's technology-based outreach efforts.

Find the full report at www.rand.org/pubs/research_reports/RR2686

Using Social Media and Social Network Analysis in Law Enforcement: Creating a Research Agenda, Including Business Cases, Protections, and Technology Needs

John S. Hollywood, Michael J. D. Vermeer, Dulani Woods, Sean E. Goodison, and Brian A. Jackson

RR-2301-NIJ (2018)

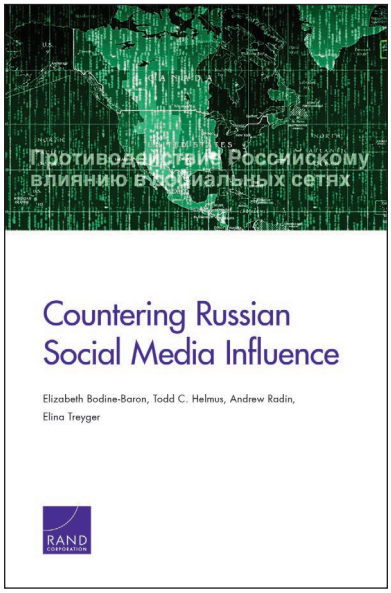
In April 2017, the National Institute of Justice convened an expert panel to identify high-priority needs for law enforcement's use of social media and social network analysis. The panel characterized business cases for employing social media and social network analysis in law enforcement, including monitoring for short-term safety threats in postings; identifying those at high risk of involvement in violence, either acutely or chronically; and investigating specific crimes and organized crime networks. The panel also specified a core case not to do: monitoring of First Amendment–protected activity for vague purposes. The panel next specified a framework for providing computer security, privacy, and civil rights protections when employing these types of analysis. The framework includes data protections for ensuring legal backings and information security; analytic protections for ensuring protection of findings, legal backing, and equitable justice outcomes; and protections on enforcement actions to ensure consistent and equitable actions and outcomes. Finally, the panel identified and prioritized needs for innovation related to social media and social network analysis. The first part of the resulting innovation agenda concerns developing policies and strategies, including best practices for transparency, collaborative decisionmaking with communities, and model policies. The second part is technical development, starting with assessing tools and how they might be better tailored to law enforcement. The third part concerns law enforcement–specific training, starting with assessing gaps in training. Training on legal issues is a short-term priority. The final part is the creation of a help desk to help law enforcement agencies navigate requests to social media companies and interpret the resulting data.

Find the full report at www.rand.org/pubs/research_reports/RR2301

Countering Russian Social Media Influence

Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger

RR-2740-RC (2018)

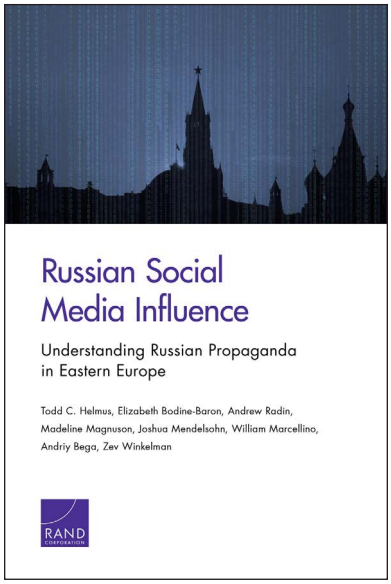


In January 2017, the U.S. intelligence community released a public report detailing a Russian influence campaign, ordered by Russian President Vladimir Putin, to disrupt the U.S. presidential election. Part of a larger multifaceted approach, this campaign included social media–based disinformation spread by both automated bots and paid trolls. Russia's strategy was to push several conflicting narratives simultaneously, deepening existing divisions within American society and degrading trust in Western institutions and the democratic process. Although it is unknown what impact the campaign might have had on the 2016 presidential election, or on individual opinions, it is clear that Russia's efforts reached many Americans through a variety of social media platforms, including Twitter and Facebook. The Russian "disinformation

chain" that directs these campaigns starts from the very top—from Russian leadership, to Russian organs and proxies, through amplification channels such as social media platforms, and finally to U.S. media consumers. This report categorizes and analyzes different approaches and policy options to respond to the specific threat of Russian influence via disinformation spread on social media in the United States. It is meant to educate and inform U.S. government officials considering policies for combating Russian disinformation; social media companies undertaking efforts to reduce the spread of disinformation on their platforms; non-governmental organizations, think tanks, and academics developing new approaches to address the threat of disinformation; and the American public.

Find the full report at www.rand.org/pubs/research_reports/RR2740

Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe



Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman

RR-2237-OSD (2018)

A RAND Corporation study examined Russian-language content on social media and the broader propaganda threat posed to the region of former Soviet states that include Estonia, Latvia, Lithuania, Ukraine, and, to a lesser extent, Moldova and Belarus. In addition to employing a state-funded multilingual television network, operating various Kremlin-supporting news websites, and working through several constellations of Russia-backed "civil society" organizations, Russia employs a sophisticated social media campaign that includes news tweets, nonattributed comments on webpages, troll and bot social media accounts, and fake hashtag and Twitter campaigns. Nowhere is this threat more tangible than in Ukraine, which has been an active propaganda battleground since the 2014 Ukrainian revolution. Other countries in the region look at Russia's actions and annexation of Crimea and recognize the need to pay careful attention to Russia's propaganda campaign. To conduct this study, RAND researchers employed a mixed-methods approach that used careful quantitative analysis of social media data to understand the scope of Russian social media campaigns combined with interviews with regional experts and U.S. and North Atlantic Treaty Organization security experts to understand the critical ingredients to countering this campaign.

Find the full report at www.rand.org/pubs/research_reports/RR2237

Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe (Testimony Presented Before the Senate Select Committee on Intelligence)

Todd C. Helmus

CT-496 (2018)

Todd Helmus shares lessons learned from the RAND study (RR-2237-OSD) in congressional testimony. Helmus provides an overview of Russian propaganda activities, reviews efforts to identify Russian propaganda on Twitter, and examines challenges confronting U.S. and European policymakers in the region. He concludes with recommendations for countering the Russian propaganda threat.

Find the full document at www.rand.org/pubs/testimonies/CT496

Russia's Use of Media and Information Operations in Turkey: Implications for the United States

Katherine Costello

PE-278-A (2018)

Russian media have sought to undermine Turkey's political and security cooperation with the United States and Europe by exacerbating mutual skepticism and highlighting policy differences. In Turkey, Russian media have also contributed to anti-American discourse and have reinforced and informed the Turkish government's own propaganda pursuits. This analysis assesses how Russia has used media and information operations to pursue its foreign policy goals related to Turkey. It examines Russian media responses to three significant events in Turkey: (1) Turkey's November 2015 shootdown of a Russian military aircraft, (2) the July 2016 Turkish coup attempt, and (3) the December 2016 assassination of the Russian ambassador. Russian media efforts following these events exemplify the propaganda strategies of amplification of genuine uncertainty, creation of opportunistic fabrications, and use of multiple contradictory narratives. These strategies have supported Russian foreign policy objectives, which include undermining the North Atlantic Treaty Organization (NATO) and fomenting mutual suspicion between Turkey and its Western allies; enlisting Ankara's support and impeding its opposition to Russian actions in Eurasia and the Middle East; and influencing Turkish internal political developments to make Turkey a more compliant partner. The U.S. government, NATO, and independent media watch groups should take steps to monitor Russian media efforts in Turkey and outside coverage of Turkey. In addition, the U.S. government, other governments, and media watch groups should continue to monitor Turkish government efforts to stifle independent media in the country and to create a propaganda arm that might emulate well-honed Russian practices.

Find the full document at www.rand.org/pubs/perspectives/PE278

Empowering ISIS Opponents on Twitter

Todd C. Helmus and Elizabeth Bodine-Baron

PE-227-RC (2017)

This Perspective presents options for operationalizing recent RAND Corporation findings about ISIS opponents and supporters on Twitter. This paper formulates a countermessaging approach for two main communication pathways. First, the authors articulate an approach for working with influential Twitter users in the Arab world to promote bottom-up and authentic counter-ISIS messaging. Second, they highlight ways that U.S. and partner governments and nongovernmental organizations can use our analysis to implement top-down messaging more effectively to directly counter ISIS support on Twitter. The original study found that there are six times the number of ISIS opponents than there are supporters on Twitter. They argue that it is critical to empower these influencers by drawing on lessons from the commercial marketing industry. They consequently highlight approaches to identify influencers on social media and empower them with both training and influential content.


RAND CORPORATION

Perspective

Expert insights on a timely policy issue

Empowering ISIS Opponents on Twitter

Todd C. Helmus, Elizabeth Bodine-Baron

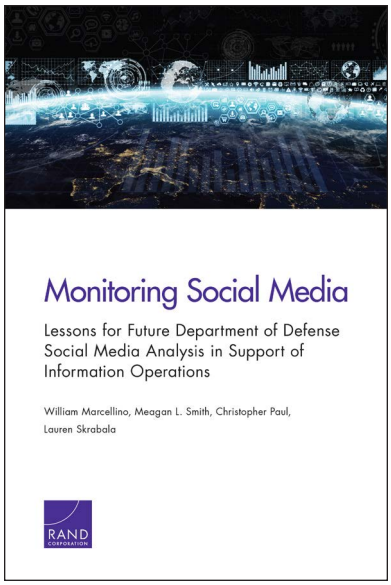
Despite recent losses on the battlefields in Syria and Iraq, the Islamic State (ISIS) remains a potent threat as it continues to gain followers and inspire terrorist attacks in the West and around the world. Social-media platforms, such as Twitter, have played a critical role in the success of ISIS, as it has used these channels to propagate its message, connect with new and established audiences, and encourage attacks. In 2015, the RAND Corporation funded a study to examine the networks of ISIS supporters and opponents on Twitter, the results of which were published in 2016.[1] That study found that, despite overwhelming numbers, opponents to ISIS are deeply fractured along both sectarian and national lines, while ISIS supporters, though fewer in number, are more coordinated and sophisticated in their use of social media.

In our previous analysis of more than 23 million tweets from more than 770,000 different user accounts from July 2014 through May 2015, we found that ISIS opponents outnumbered supporters six to one, with that ratio growing to 30 to one toward the end of May 2015. Unfortunately, despite the larger number of opponents, ISIS supporters are still perceived to dominate Twitter. This perception is based in part on the fact that ISIS supporters routinely "out-tweet" opponents, as they on average produce 50 percent more daily tweets. Furthermore, they employ sophisticated social-media strategies, mobilizing their followers to spread their content quickly and effectively. For example, ISIS media offices produce content tailored to many different audiences in different languages, ranging from simple text to highly produced, almost theatrical videos. Their tweets routinely include phrases such as "breaking news," "spread," "link," "now released," and "pictorial content," terms that are missing from the ISIS opposition tweets.

Opponents to ISIS, on the other hand, are divided along both sectarian and national lines. Drawing on network and lexical analysis, we discovered four large metacommunities: three mostly opposing ISIS (Sunni, Shia, and Syrian mujahideen) and one sup-

Find the full document at www.rand.org/pubs/perspectives/PE227

Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations



William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala

RR-1742-OSD (2017)

Social media analysis is playing an important and increasing role in advertising and academic research, but it also has significant potential to support military information operations by providing a window into the perspectives, thoughts, and communications of a wide range of relevant audiences. Although there are compelling national security reasons to field a social media analysis capability, the U.S. Department of Defense (DoD) must do so while navigating U.S. law and cultural norms and under conditions of great uncertainty. Existing legal and policy frameworks have not anticipated the rapid pace and global reach of modern communication networks, and questions of cost and implementation hinder the development of a robust social media analysis capability and the most fruitful applications for these analyses. To support DoD's assessment of the benefits, trade-offs, and implementation challenges that it will face as it expands its capacity for social media analysis, this report reviews the analytic approaches that will be most valuable for information operations, as well as legal, ethical, policy, technological, and training considerations. It also includes a set of recommendations to help DoD navigate this terrain while building a robust, effective social media analysis capability to support operations worldwide.

Find the full report at www.rand.org/pubs/research_reports/RR1742

The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It

Christopher Paul and Miriam Matthews

PE-198-OSD (2016)

The authors characterize the contemporary Russian model for propaganda as "the firehose of falsehood" because of two of its distinctive features: high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions. In the words of one observer, "[N]ew Russian propaganda entertains, confuses and overwhelms the audience."

Contemporary Russian propaganda has at least two other distinctive features. It is rapid, continuous, and repetitive, and it lacks commitment to consistency. Interestingly, several of these features run directly counter to the conventional wisdom on effective influence and communication from government or defense sources, which traditionally emphasize the importance of truth, credibility, and the avoidance of contradiction. Despite ignoring these traditional principles, Russia seems to have enjoyed some success under its contemporary propaganda model, either through more direct persuasion and influence or by engaging in obfuscation, confusion, and the disruption or diminution of truthful reporting and messaging. The authors offer several possible explanations for the effectiveness of Russia's firehose of falsehood. These observations draw from a concise, but not exhaustive, review of the literature on influence and persuasion, as well as experimental research from the field of psychology. They explore the four identified features of the Russian propaganda model and show how and under what circumstances each might contribute to effectiveness. Many

successful aspects of Russian propaganda have surprising foundations in the psychology literature, so the authors conclude with a brief discussion of possible approaches from the same field for responding to or competing with such an approach.

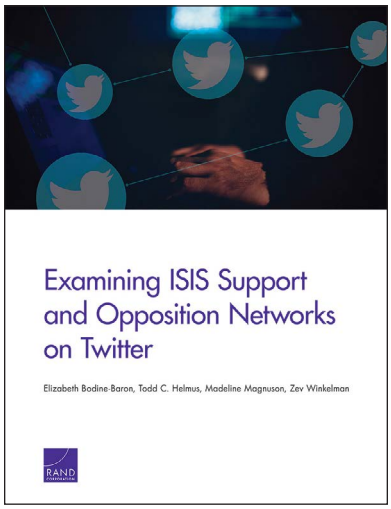
Find the full document at www.rand.org/pubs/perspectives/PE198

Examining ISIS Support and Opposition Networks on Twitter

Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, and Zev Winkelman

RR-1328-RC (2016)

The Islamic State in Iraq and Syria (ISIS), like no other terrorist organization before, has used Twitter and other social media channels to broadcast its message, inspire followers, and recruit new fighters. Although much less heralded, ISIS opponents have also taken to Twitter to castigate the ISIS message. This report draws on publicly available Twitter data to examine this ongoing debate about ISIS on Arabic Twitter and to better understand the networks of ISIS supporters and opponents on Twitter. To support the countermessaging effort and to more deeply understand ISIS supporters and opponents, this study uses a mixed-methods analytic approach to identify and characterize in detail both ISIS support and opposition networks on Twitter. This analytic approach draws on community detection algorithms that help detect interactive communities of Twitter users, lexical analysis that can identify key themes and content for large data sets, and social network analysis.



Find the full report at www.rand.org/pubs/research_reports/RR1328

DATA ANALYTICS

Leveraging Big Data Analytics to Improve Military Recruiting

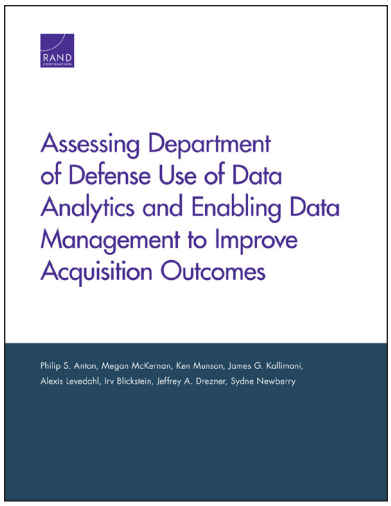
Nelson Lim, Bruce R. Orvis, and Kimberly Curry Hall

RR-2621-OSD (2019)

The authors identified ways that the U.S. Department of Defense (DoD) and the services might be able to further deploy data-driven outreach and recruiting strategies in their outreach and recruiting processes. Their report summarizes information collected from stakeholders, subject-matter experts (SMEs), and the literature. The authors convened an advisory group of representatives from the services' recruiting operations divisions and marketing programs. The advisory group shared information on strategies, practices, policies, databases, algorithms, and tools. The authors also identified and convened a group of DoD Privacy Program and personally identifiable information SMEs to discuss the DoD Privacy Program, including related restrictions on data-enabled outreach and recruiting. Additionally, they conducted focus groups with military recruiters concerning recruiting practices and challenges at the local level and reviewed business and academic literature describing use of data-enabled practices in marketing and recruiting. The authors discuss barriers that must be overcome and provide actions that DoD can take toward enhancing use of data-enabled recruiting practices; these include evaluating the efficacy and efficiency of such practices.

Find the full report at www.rand.org/pubs/research_reports/RR2621

Assessing Department of Defense Use of Data Analytics and Enabling Data Management to Improve Acquisition Outcomes



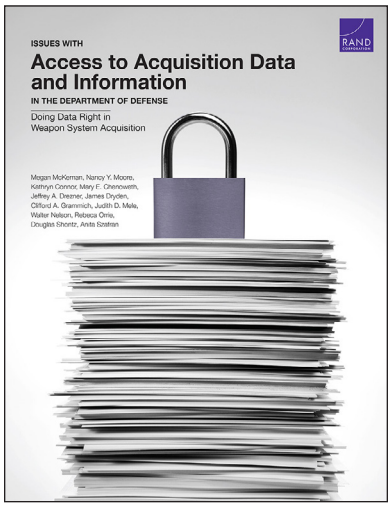
Philip S. Anton, Megan McKernan, Ken Munson, James G. Kallimani, Alexis Levedahl, Irv Blickstein, Jeffrey A. Drezner, and Sydne Newberry

RR-3136-OSD (2019)

In the conference report accompanying the National Defense Authorization Act for Fiscal Year 2017, Congress expressed concern that the U.S. Department of Defense (DoD) "does not sufficiently incorporate data into its acquisition-related learning and decision-making" and asked six questions about "the use of data analysis, measurement, and other evaluation-related methods in DoD acquisition programs." In this report, the authors decompose and measure acquisition functions, data governance, and training to assess how data and associated analytics support DoD acquisition decisionmaking. The authors found that DoD is applying a breadth of data analytics to acquisition. Capabilities range from simple data archives and plotting to archives integrated with commercial analytic tools. DoD has implemented an array of data governance and management practices, but major challenges remain, including a culture against data sharing and concerns about security and oversight burden. Some commercial breakthroughs in advanced analytics sound promising for DoD acquisition, but some might not be applicable; research is ongoing. Advancement should include developing a data analytics strategy across acquisition domains, expanding data governance and data sharing, and continuing to expand and mature data collection, access, and analytic layers. Also, mechanisms are needed to authorize and ensure protected access to data for both the DoD and external analysts. Improved incentives and understanding of data analytics could encourage decisionmakers to make better use of capabilities.

Find the full report at www.rand.org/pubs/research_reports/RR3136

Issues with Access to Acquisition Data and Information in the Department of Defense: Doing Data Right in Weapon System Acquisition



Megan McKernan, Nancy Y. Moore, Kathryn Connor, Mary E. Chenoweth, Jeffrey A. Drezner, James Dryden, Clifford A. Grammich, Judith D. Mele, Walter Nelson, Rebeca Orrie, Douglas Shontz, and Anita Szafran

RR-1534-OSD (2017)

Acquisition data and information are the foundation for decisionmaking, management, and oversight of weapon-system acquisition programs. They are critical to initiatives to improve defense acquisition, such as Better Buying Power. The Department of Defense as a whole gathers a wide variety of acquisition information and stores it in multiple, sometimes incompatible systems, most of which are built for reporting, not analysis. Large businesses have similar problems, and the concept of master data management might have lessons for both. The authors review 21 key acquisition-related data information systems and their

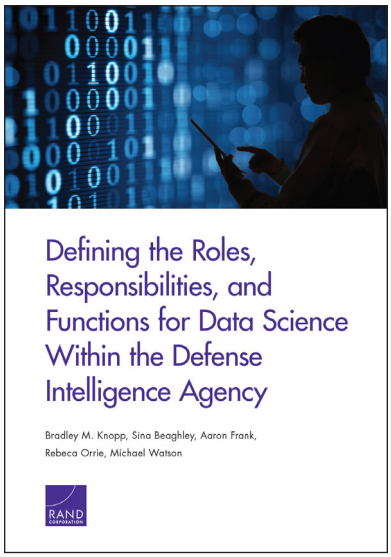
origins and uses, and identify how acquisition data might be improved. They also summarize background on acquisition data; review commercial practices in data management; and offer findings and recommendations to further improve acquisition data quality, access, and use.

Find the full report at www.rand.org/pubs/research_reports/RR1534

Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency

Bradley M. Knopp, Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson

RR-1582-DIA (2016)



This report addresses and recommends potential methods for the Defense Intelligence Agency (DIA) to identify, hire, and organize data scientists. The authors examine data science activities in the private sector and university-level data science training and explore hiring and retention options for creating a data science capability within DIA. They also examine the results of interviews with DIA employees. The authors recommend that DIA create its own data science capability with a mix of government experts and contractors capable of managing activities unique to military intelligence operations and that DIA establish a center of excellence to oversee and promote data science activities, development, and training.

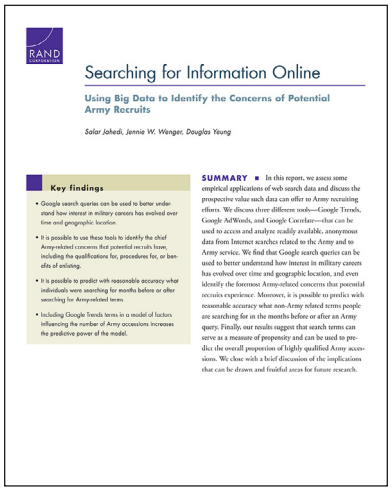
Find the full report at www.rand.org/pubs/research_reports/RR1582

Searching for Information Online: Using Big Data to Identify the Concerns of Potential Army Recruits

Salar Jahedi, Jennie W. Wenger, and Douglas Yeung

RR-1197-A (2016)

This report assesses empirical applications of web search data and discusses the prospective value such data can offer Army recruiting efforts. The authors examine three different tools—Google Trends, Google AdWords, and Google Correlate—that can be used to access and analyze readily available, anonymous data from internet searches related to the Army and to Army service. They found that Google search queries can inform how interest in military careers has evolved over time and by geographic location and can identify the foremost Army-related concerns that potential recruits have. Moreover, by analyzing how search terms correlate across time, it is possible to predict with reasonable accuracy what non-Army related terms people are searching for in the months before or after an Army query. These queries serve as leading and lagging indicators of Army-related searches and can offer a glimpse into the concerns of individuals near the period when they are considering joining. The results suggest that search terms can serve as an indicator of propensity and can be incorporated into models to predict highly qualified Army accessions.



Find the full report at www.rand.org/pubs/research_reports/RR1197

Issues with Access to Acquisition Data and Information in the Department of Defense

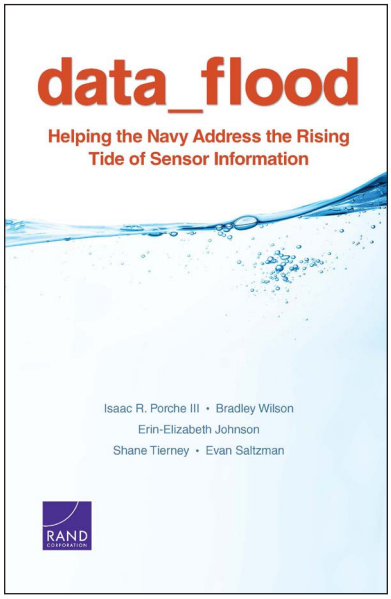
Jessie Riposo, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar, and Jerry M. Sollinger

RR-880/1-OSD (2015)

Acquisition data underpin the management and oversight of the U.S. defense acquisition portfolio. However, balancing security and transparency has been an ongoing challenge. Some acquisition professionals are not getting the data they need to perform their assigned duties or are not getting the data and information in an efficient manner. To help guide the Office of the Secretary of Defense (OSD) in addressing these problems, the RAND Corporation identified access problems at the OSD level—including those organizations that require access to data and information to support OSD, such as the analytic support of federally funded research and development centers and direct support contractors—and evaluated the role of policy in determining access. *Issues with Access to Acquisition Data and Information in the Department of Defense* finds that the process for gaining access to data is inefficient and might not provide access to the best data to support analysis, and that OSD analytic groups and support contractors face particular challenges in gaining access to data. Given the inherent complexity in securing data and sharing data, any solutions to problems associated with data-sharing must be well thought out to avoid the multitude of unintended consequences that could arise.

Find the full report at www.rand.org/pubs/research_reports/RR880z1

Data Flood: Helping the Navy Address the Rising Tide of Sensor Information



Isaac R. Porche III, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman

RR-315-NAVY (2014)

In the U.S. Navy, there is a growing demand for intelligence, surveillance, and reconnaissance (ISR) data, which help Navy commanders obtain situational awareness and help Navy vessels perform a host of mission-critical tasks. However, the amount of data generated by ISR sensors has become overwhelming, and Navy analysts are struggling to keep pace with this data flood. Their challenges include extremely slow download times, workstations cluttered with applications, and stovepiped databases and networks—challenges that are only going to intensify as the Navy fields new and additional sensors in the coming years. Indeed, if the Navy does not change the way it collects, processes, exploits, and disseminates information, it will reach an ISR *tipping point*—the point at which its analysts are no longer able to complete a minimum number of exploitation tasks within given time constraints—as soon as 2016. The authors explore options for solving the Navy's big data challenge, considering changes across four dimensions: people, tools and technology, data and data architectures, and demand and demand management. They recommend that the Navy pursue a cloud solution—a strategy similar to those adopted by Google, the intelligence community, and other large organizations grappling with big data's challenges and opportunities.

Find the full report at www.rand.org/pubs/research_reports/RR315

Cost Considerations in Cloud Computing

Kathryn Connor, Ian P. Cook, Isaac R. Porche III, and Daniel Gonzales

PE-113-A (2014)

Cloud computing has garnered the attention of the Department of Defense (DoD) as data and computer processing needs grow and budgets shrink. Programs are interested in the potential of cloud computing to control growing data management costs, but reliable literature on the costs of cloud computing in the government is still limited. Researchers found that cloud provider costs can vary in value compared with traditional information system alternatives because of cost structure variations. They analyzed the cost drivers for several data management approaches for one acquisition program to develop structured cost considerations for analysts evaluating new cloud investments. These considerations can help analysts be comprehensive in their analysis until DoD develops official guidance on cloud computing cost analysis.

Find the full document at www.rand.org/pubs/perspectives/PE113

Ramifications of DARPA's Programming Computation on Encrypted Data Program

Martin C. Libicki, Olesya Tkacheva, Chaoling Feng, and Brett Hemenway

RR-567-OSD (2014)

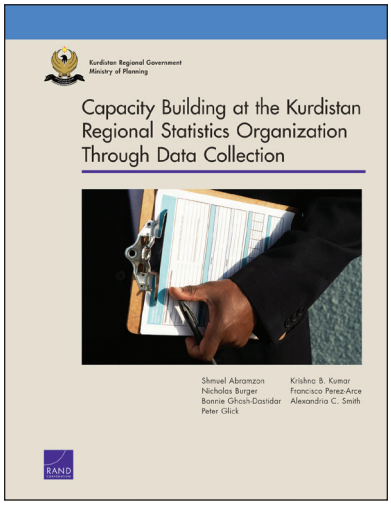
Programming Computation on Encrypted Data (PROCEED) is a Defense Advanced Research Projects Agency program whose primary purpose is to improve the efficiency of algorithms that allow people to carry out computations on encrypted data—without having to decrypt the data itself. RAND was asked to evaluate whether PROCEED—which expands the knowledge base of the global cryptographic community—is likely to provide more benefits to the United States than it does to its global rivals. The research team's assessment focused on the degree to which PROCEED technologies might be adopted, under what circumstances, and for what purpose. The team then used the analytic framework generated to understand technological uptake decisions as a way of ascertaining how such factors would work in Russia and China vis-à-vis the United States (and, by extension, countries similar to the United States).

Find the full report at www.rand.org/pubs/research_reports/RR567

Capacity Building at the Kurdistan Region Statistics Office Through Data Collection

Shmuel Abramzon, Nicholas Burger, Bonnie Ghosh-Dastidar, Peter Glick, Krishna B. Kumar, Francisco Perez-Arce, and Alexandria C. Smith

RR-293-KRG (2014)



Comprehensive and reliable statistics are crucial for designing economic policies. The Kurdistan Region of Iraq lacks the statistics it needs to improve infrastructure, encourage private-sector development, attract foreign investment, and create sustained economic growth. The Kurdistan Region Statistics Office needs to build capacity to collect the data. RAND worked closely with the office and in consultation with relevant ministries to build capacity by preparing, conducting, and

analyzing the first round of a survey of the region's labor force critical to government policymaking. RAND provided overall guidance and both analytical and hands-on training to organization staff. Furthermore, by being involved in the complete life cycle of the survey, from conception through data collection to policy analysis, and by being responsible for the final execution and analysis of the surveys, that staff benefited from learning by doing. Future rounds of the survey will provide up-to-date information on how these and other important indicators are changing over time and in response to policies.

Translated Arabic and Kurdish versions were also published.

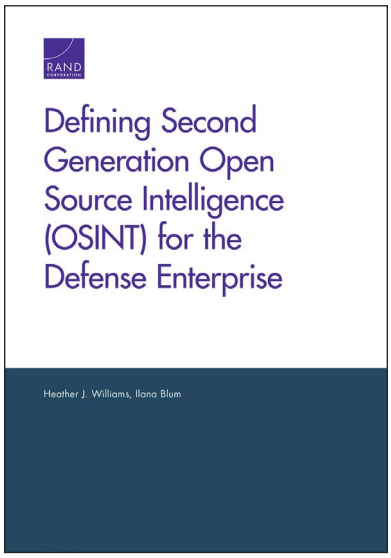
Find the full report at www.rand.org/pubs/research_reports/RR293

Find the Arabic report at www.rand.org/pubs/research_reports/RR293z2

Find the Kurdish report at www.rand.org/pubs/research_reports/RR293z3

INTELLIGENCE COLLECTION AND ANALYSIS

Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise



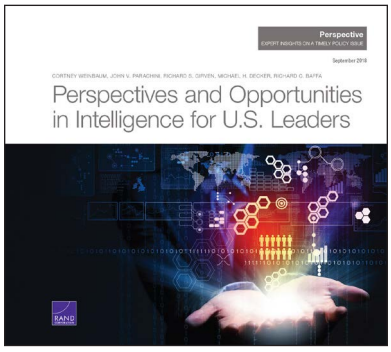
Heather J. Williams and Ilana Blum

RR-1964-OSD (2018)

This report presents a framework for understanding the modern practice of open source intelligence. It reviews the literature on open source intelligence and reexamines definitions used in other areas by the U.S. intelligence community in the context of modern open source information. The report describes the evolution of open source intelligence over the past 50-plus years, defines open source information and the open source intelligence cycle, and draws parallels between open source as an intelligence discipline and other intelligence disciplines. It also examines the methods used by open source tools and the challenges of using off-the-shelf technology for open source analysis. It concludes by suggesting areas for further study.

Find the full report at www.rand.org/pubs/research_reports/RR1964

Perspectives and Opportunities in Intelligence for U.S. Leaders



Cortney Weinbaum, John V. Parachini, Richard S. Girven, Michael H. Decker, and Richard C. Baffa

PE-287-OSD (2018)

Threats to the international order from near-peer competitors and from rogue regimes, terrorists, and the proliferation of cyberweapons and weapons of mass destruction all challenge whether the U.S. intelligence community (IC) will be able to fulfill its mission. It is unclear whether

the IC is prepared to provide decisionmakers and warfighters with the intelligence they need and expect. This Perspective presents five distinct discussions of changes the IC can make to meet these challenges in the areas of strategic warning; tasking, collection, processing, exploitation, and dissemination (TCPED); security, counterintelligence, and insider threats; open-source information; and surging for crises. Each of the five discussions in this Perspective provides analysis and recommendations that might be read, acted on, and implemented alone—but the authors believe that the IC has an opportunity to make a major leap forward by acting in a coordinated manner on all five of the topics together.

Find the full document at www.rand.org/pubs/perspectives/PE287

Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community

Stephen Artner, Richard S. Girven, and James B. Bruce

RR-1408-OSD (2016)

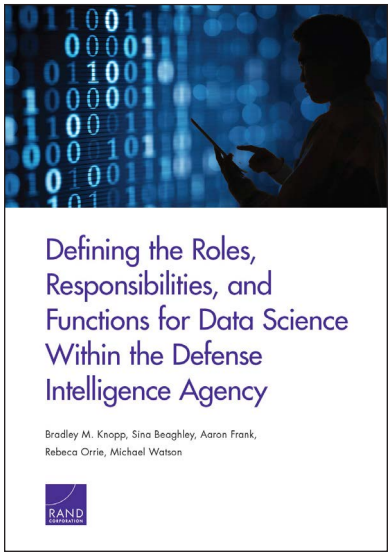
Structured analytic techniques (SATs) are a key part of the rigorous analytic tradecraft the intelligence community (IC) has pursued in recent years, but so far these techniques have received little systematic evaluation. This report argues that the assessment of SATs is essential, albeit difficult; suggests specific questions that should be part of that assessment; and proposes several methods for ascertaining the practical value of SATs. The report also offers the results of a pilot study that explored conducting such an evaluation via structured interviews with analytic practitioners and a qualitative assessment of a body of IC products to examine the incidence and utility of SATs. These preliminary efforts do not offer definitive conclusions about the value of SATs but illustrate how the IC might evaluate them more systematically.

Find the full report at www.rand.org/pubs/research_reports/RR1408

Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency

Bradley M. Knopp, Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson

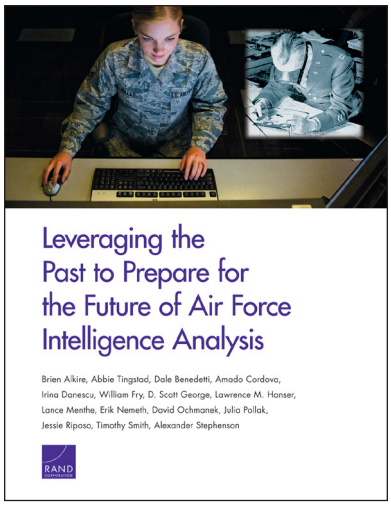
RR-1582-DIA (2016)



This report addresses and recommends potential methods for the Defense Intelligence Agency (DIA) to identify, hire, and organize data scientists. The authors examine data science activities in the private sector and university-level data science training and explore hiring and retention options for creating a data science capability within DIA. They also examine the results of interviews with DIA employees. The authors recommend that DIA create its own data science capability with a mix of government experts and contractors capable of managing activities unique to military intelligence operations and that DIA establish a center of excellence to oversee and promote data science activities, development, and training.

Find the full report at www.rand.org/pubs/research_reports/RR1582

Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis



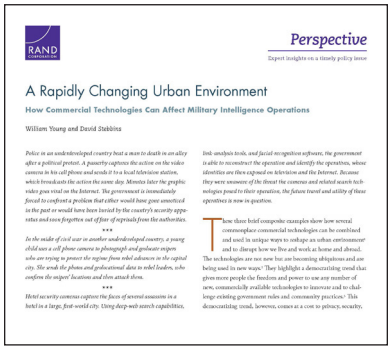
Brien Alkire, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Danescu, William Fry, D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie Riposo, Timothy Smith, and Alexander Stephenson

RR-1330-AF (2016)

This report describes steps the U.S. Air Force can take to help ensure that it has the capability needed to provide intelligence analysis support to a broad range of service and combatant commander needs, including support to ongoing irregular warfare operations, and to conventional warfare with a near-peer competitor. It describes lessons from past operations that have direct implications for Air Force intelligence analysis or that Air Force intelligence analysis could help to address. It also describes future challenges for Air Force intelligence analysis. It makes recommendations related to doctrine, training and career field development, analysis tools, and processes that can help to address the lessons from the past and prepare Air Force intelligence analysts for the challenges of the future.

Find the full report at www.rand.org/pubs/research_reports/RR1330

A Rapidly Changing Urban Environment: How Commercial Technologies Can Affect Military Intelligence Operations



William Young and David Stebbins

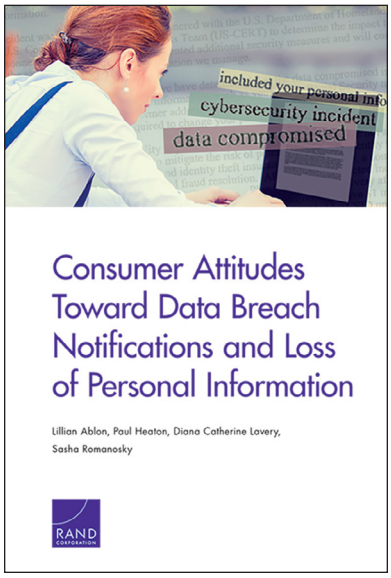
PE-181-OSD (2016)

Commonplace commercial technologies can be combined and used in unique ways to reshape an urban environment and disrupt how we live and work, in the United States and abroad. The technologies are not new but are becoming ubiquitous and are being used in new ways. The technologies highlight a democratizing trend that gives more people the freedom and power to use any number of new, commercially available technologies to innovate and to challenge existing government rules and community practices. However, this democratizing trend comes at a cost to privacy, security, and secrecy and is changing the way people interact socially and politically. It is changing the way we conduct business, diplomacy, intelligence operations, and war, the future of which is likely to be increasingly urban in nature.

Find the full document at www.rand.org/pubs/perspectives/PE181

INFORMATION SECURITY AND PRIVACY

Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information



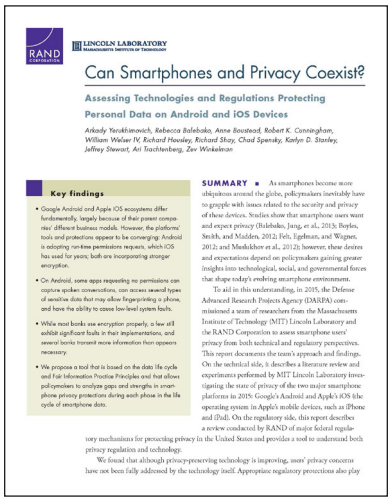
Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky

RR-1187-ICJ (2016)

Data breaches continue to plague private-sector companies, nonprofit organizations, and government agencies. Despite the mounting rate of these breaches, the continuing harms imposed on consumers and firms, and over a decade of breach notification laws, very little research exists that examines consumer response to these developments. This report sets out the results of a nationally representative survey of the consumer experience with data breaches: the frequency of notifications of data breaches and the type of data taken; consumer attitudes toward data breaches, breach notifications, and company follow-on responses; and perceived personal costs resulting from the breach, with the goal to establish a baseline of information about consumer attitudes toward data loss and company practices in responding to such events. Key findings include: (1) Twenty-six percent of respondents, or an estimated 64 million U.S. adults, recalled a breach notification in the past 12 months; (2) 44 percent of those notified were already aware of the breach; (3) 62 percent of respondents accepted offers of free credit monitoring; (4) only 11 percent of respondents stopped dealing with the affected company following a breach; (5) 32 percent of respondents reported no costs of the breach and any inconvenience it garnered, while, among those reporting some cost, the median cost was $500; and (6) 77 percent of respondents were highly satisfied with the company's postbreach response.

Find the full report at www.rand.org/pubs/research_reports/RR1187

Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices



Arkady Yerukhimovich, Rebecca Balebako, Anne E. Boustead, Robert K. Cunningham, William Welser IV, Richard Housley, Richard Shay, Chad Spensky, Karlyn D. Stanley, Jeffrey Stewart, Ari Trachtenberg, and Zev Winkelman

RR-1393-DARPA (2016)

As smartphones become more ubiquitous around the globe, policymakers inevitably have to grapple with issues related to the security and privacy of these devices. To aid in this understanding, in 2015, the Defense Advanced Research Projects Agency commissioned a team of researchers from the Massachusetts Institute of Technology (MIT) Lincoln Laboratory and the RAND Corporation to assess smartphone users' privacy from both technical and regulatory perspectives. This report documents the

team's approach and findings. On the technical side, it describes a literature review and experiments performed by MIT Lincoln Laboratory investigating the state of privacy of the two major smartphone platforms in 2015: Google's Android and Apple's iOS. On the regulatory side, this report describes a review by RAND of major federal regulatory mechanisms for protecting privacy in the United States and provides a tool to understand both privacy regulation and technology.

Find the full report at www.rand.org/pubs/research_reports/RR1393

Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law

Edward Balkovich, Don Prosnitz, Anne Boustead, and Steven C. Isley

RR-800-NIJ (2015)

Mobile phones, the networks they connect to, the applications they use, and the services they access all collect and retain enormous amounts of information that can be useful in criminal investigations. However, state and local law enforcement face two substantial challenges when accessing these data: (1) maintaining awareness of the sources and nature of commercial data available to an investigator and (2) determining the legal rules for access to these data. This report explores these issues and describes the development of a prototype tool—the Mobile Information and Knowledge Ecosystem—intended to help law enforcement, commercial entities, and policy analysts explore the mobile ecosystem and understand the laws regulating law enforcement's use of data contained within the mobile ecosystem. The tool might also serve as a mechanism for sharing best practices in electronic surveillance.

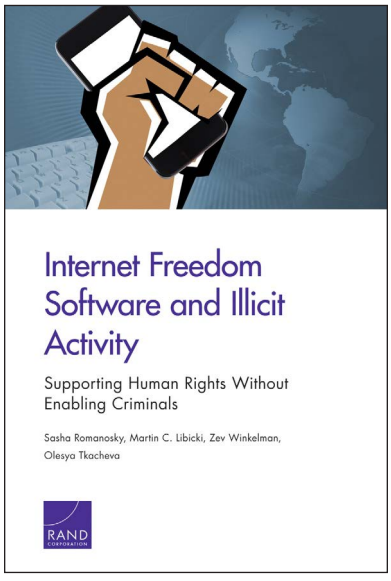
Find the full report at www.rand.org/pubs/research_reports/RR800

Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals

Sasha Romanosky, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva

RR-1151-DOS (2015)

The State Department's Bureau of Democracy, Human Rights, and Labor (DRL), as part of its broader effort to protect and advance political and economic freedoms and human rights, champions the United States' strategy for cyberspace to advocate for fundamental freedoms of speech and association through cyberspace; empower civil society actors, human rights activists, and journalists in their use of digital media; and encourage governments to limit neither the freedom of expression nor the free flow of information. To this end, DRL funds the development of many cybersecurity and privacy software programs. However, there are trade-offs associated with any such investment. On one hand, security and privacy tools can provide safe, reliable, and anonymous internet access to people who would otherwise be censored, filtered, or punished for communicating electronically. On the other hand, these tools could also be used to conceal or commit illegal activity. This report examines the portfolio of tools funded by DRL that help support internet freedom and assesses the impact of these tools in promoting U.S. interests. First, the authors note the benefits of these tools in promoting DRL's mission of internet freedom across the world. Second, they examine their potential for, and examples of, their illicit use. Third, they consider the ability of comparable tools, not funded by the DRL, to be used for such purposes. And fourth, they examine safeguards and design and service models



that could limit or restrict the use of the technologies for illicit purposes. The report concludes that DRL's support for internet freedom tools has not made them more likely to be used for illicit purposes, relative to alternative technologies not funded by DRL.

Find the full report at www.rand.org/pubs/research_reports/RR1151

Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies

Neil Robinson and Jan Gaspers

RR-557-ME (2014)

This study reviews the legal and policy frameworks that govern the use of information and communications technology by European Union institutions and agencies in terms of the extent to which they account for information security and data privacy.

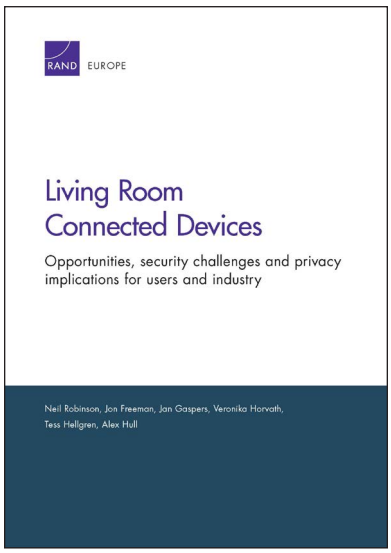
Find the full report at www.rand.org/pubs/research_reports/RR557

Living Room Connected Devices: Opportunities, Security Challenges and Privacy Implications for Users and Industry

Neil Robinson, Jon Freeman, Jan Gaspers, Veronika Horvath, Tess Hellgren, and Alex Hull

RR-604-OFCOM (2014)

RAND Europe was commissioned by Ofcom, the UK communications regulator, to investigate and prepare an independent expert report on the growth of the connected living room and the implications of this growth for UK citizens and consumers. As the living room becomes an internet connected space, this shift offers opportunities to consumers and industry while also raising potential privacy and security concerns. Although currently a nascent market, the uptake of living room connected devices is expected to grow significantly in the coming years. However, it appears that there is a low awareness of how the capabilities of living room connected devices might be used, either legitimately by industry or illegitimately by criminal actors. This report addresses the security and privacy implications of the internet connected living room for both industry and consumers, discussing potential benefits and emerging threats associated with living room connected devices and their technical capabilities.



Find the full report at www.rand.org/pubs/research_reports/RR604

Portfolio Assessment of the Department of State Internet Freedom Program

Ryan Henry, Stacie L. Pettyjohn, and Erin York

RR-794-DOS (2014)

The struggle between those promoting internet freedom and those trying to control and monitor the internet is a fast-paced game of cat and mouse, and the State Department's Bureau of Democracy, Human Rights, and Labor (DRL) internet freedom program seeks to fund projects that promote preserving the open character of the internet. Employing portfolio analysis techniques, the authors assessed DRL's internet freedom portfolio

for fiscal year 2012–2013. The assessment showed good alignment between the State Department's strategy and the cumulative effect of the 18 funded projects. Additionally, the portfolio was assessed to be well balanced with an unrealized potential for supporting emergent State Department needs in enlarging political space within authoritarian regimes. The assessment revealed that the investment in developing internet freedom capacity and capabilities would likely have residual value beyond the portfolio's funded lifespan, with positive but indirect connections to civic freedom. Moreover, promoting internet freedom appears to be a cost-imposing strategy that simultaneously aligns well with both U.S. values and interests, pressuring authoritarian rivals to either accept a free and open internet or devote additional security resources to control or repress internet activities. Finally, the authors determined that the value of such analysis is best realized over multiple stages of the portfolio's life cycle. Among the authors' recommendations were for DRL to enhance the synergy within the portfolio and among its grantees and to maintain a relatively balanced internet freedom strategy that includes projects working on access, anonymity, awareness, and advocacy.

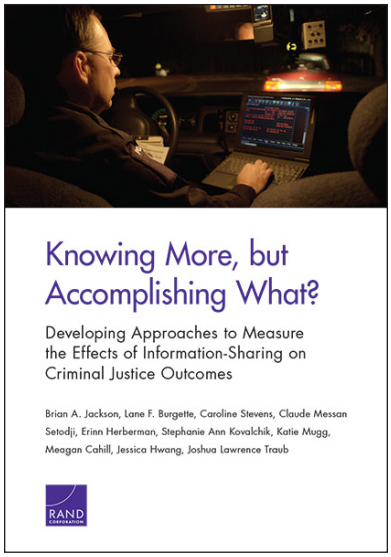
Find the full report at www.rand.org/pubs/research_reports/RR794

INFORMATION-SHARING

Knowing More, but Accomplishing What? Developing Approaches to Measure the Effects of Information-Sharing on Criminal Justice Outcomes

Brian A. Jackson, Lane F. Burgette, Caroline Stevens, Claude Messan Setodji, Erinn Herberman, Stephanie Ann Kovalchik, Katie Mugg, Meagan Cahill, Jessica Hwang, and Joshua Lawrence Traub

RR-2099-NIJ (2017)



Information-sharing became a central element of the policy debate about U.S. homeland and national security after the September 11, 2001, terrorist attacks. However, sharing of information across jurisdictional lines is just as important for everyday criminal justice efforts to prevent and investigate crime, and systems to provide such capabilities have been in place for many years. Despite widespread belief that information-sharing is valuable, there have been relatively limited efforts to measure its effect on criminal justice outcomes. To help address this need, the authors examined the measurement of information-sharing effects from the strategic to the tactical levels, with a focus on developing reliable measurements that capture the range of ways sharing can affect outcomes and how the practicalities of law enforcement work practices can affect measurement. In collaboration with an advanced regional information-sharing agency, the authors developed techniques to examine the effects of multiple types of data-sharing at the officer, case, and offender levels. Analyses showed significant correlations between different types of sharing on the level of interagency involvement in cases for individual offenders, on the timing and likelihood of specific law enforcement events, and on the likelihood of individual police officers to be involved in cross-jurisdictional arrests. In addition, the authors explored lessons for future policy evaluation and information system design to facilitate measurement.

Find the full report at www.rand.org/pubs/research_reports/RR2099

Improving Information-Sharing Across Law Enforcement: Why Can't We Know?

John S. Hollywood and Zev Winkelman

RR-645-NIJ (2015)

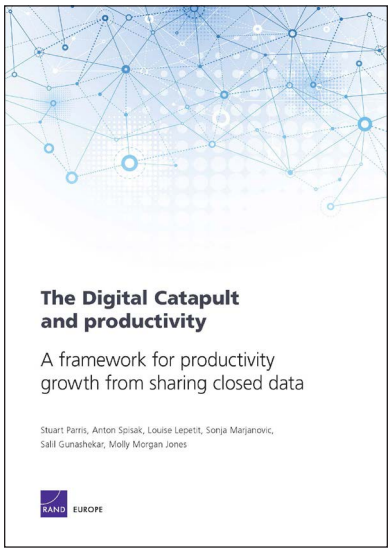
Law enforcement capabilities increasingly depend on records management systems (RMSs) that maintain agencies' case histories, computer-aided dispatch (CAD) systems that maintain agencies' calls for service and call response histories, and other data systems. There are also increasing demands to share information with regional, state, and federal repositories of criminal justice information. A good deal of progress has been made on developing information-sharing standards, developing repositories of shared law enforcement information, developing common policies, and improving affordability. However, there are limitations with respect to existing information-sharing technology and policy. Commercial providers can have business models that do not support greater and cheaper information-sharing. Widespread concerns remain regarding the cost of RMSs, CAD, and other key systems. To address these barriers in the short term, the authors have identified information-sharing items to include in requests for proposals (RFPs). They identify indicators that can help agencies determine whether bidding providers are interested in supporting information-sharing at comparatively low costs, and they provide some tips on writing requirements and pursuing new, lower-cost business models. In the longer term, they discuss building on existing developments to create a comprehensive framework for information-sharing. They identify critical interfaces that have not been captured. They present elements to be included in model policy and RFP language related to information-sharing, information assurance, and privacy and civil rights. Finally, they recommend further support for the new technology and business models that can help make these systems more affordable.

Find the full report at www.rand.org/pubs/research_reports/RR645

The Digital Catapult and Productivity: A Framework for Productivity Growth from Sharing Closed Data

Stuart Parris, Anton Spisak, Louise Lepetit, Sonja Marjanovic, Salil Gunashekar, and Molly Morgan Jones

RR-1284-DC (2015)



The Digital Catapult is a national center designed to advance rapidly the UK's best digital ideas and to help unlock new value from sharing closed and proprietary data. RAND Europe was commissioned by the Digital Catapult to conduct a study to develop a conceptual framework to understand the present and prospective contribution of the Digital Catapult's activities to the UK's economic productivity. The authors found that the Digital Catapult targets market and innovation inefficiencies that likely inhibit the rapid commercialization and up-take of data innovation across firms and industries. If not addressed, these barriers might well hinder the benefits that sharing closed and proprietary data sets and open innovation could deliver to productivity growth in the UK. The Digital Catapult has three main mechanisms of change through which it can unlock these efficiency barriers for different sectors, disciplines and organizational types by: (1) enabling the development of core data infrastructure; (2) increasing the absorptive capacity of organizations to derive the value from data, assimilate it and use it toward commercial ends; and (3) convening expertise, providing leadership and fostering trust in key markets.

Find the full report at www.rand.org/pubs/research_reports/RR1284

How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts

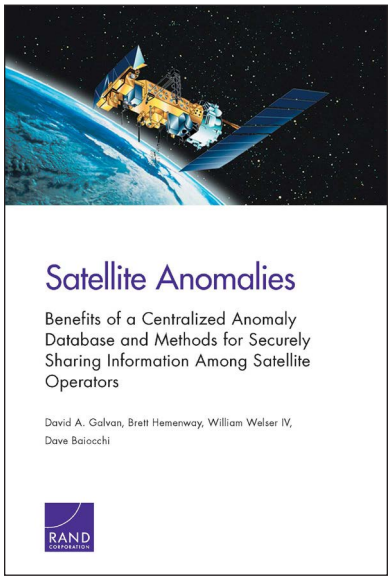
Brian A. Jackson

RR-380-OSD (2014)

Since the terrorist attacks of September 11, 2001, the sharing of intelligence and law enforcement information has been a central part of U.S. domestic security efforts. Although much of the public debate about such sharing focuses on addressing the threat of terrorism, organizations at all levels of government routinely share varied types of information through multiagency information systems, collaborative groups, and other links. Given resource constraints, there are concerns about the effectiveness of information-sharing and fusion activities and, therefore, their value relative to the public funds invested in them. However, solid methods for evaluating these efforts are lacking, limiting the ability to make informed policy decisions. Drawing on a substantial literature review and synthesis, this report lays out the challenges of evaluating information-sharing efforts that frequently seek to achieve multiple goals simultaneously; reviews past evaluations of information-sharing programs; and lays out a path to improving the evaluation of such efforts going forward.

Find the full report at www.rand.org/pubs/research_reports/RR380

Satellite Anomalies: Benefits of a Centralized Anomaly Database and Methods for Securely Sharing Information Among Satellite Operators



David A. Galvan, Brett Hemenway, William Welser IV, and Dave Baiocchi

RR-560-DARPA (2014)

This report describes the nature and causes of satellite anomalies, and the potential benefits of a shared and centralized satellite anomaly database. Findings indicate that a shared satellite anomaly database would bring significant benefits to the commercial community, and the main obstacles are reluctance to share detailed information with the broader community, as well as a lack of dedicated resources available to any trusted third party to build and manage such a database. Trusted third parties and cryptographic methods, such as secure multiparty computing or differential privacy, are not complete solutions, but show potential to be further tailored to help resolve the issue of securely sharing anomaly data.

Find the full report at www.rand.org/pubs/research_reports/RR560

Improving Interagency Information Sharing Using Technology Demonstrations: The Legal Basis for Using New Sensor Technologies for Counterdrug Operations Along the U.S. Border

Daniel Gonzales, Sarah Harting, Jason Mastbaum, and Carolyn Wong

RR-551-OSD (2014)

The Department of Defense (DoD) has developed new sensor technologies to support military forces operating in Iraq and Afghanistan. These new capabilities might be useful in counterdrug (CD) operations along the southern U.S. border. DoD has held technology demonstrations to test and demonstrate new technologies

along the southern border—because the field conditions along the border closely resemble those in current military theaters of operation and because they can also reveal whether new technologies are useful for CD operations led by domestic law enforcement agencies. However, there are legal questions about whether such technology demonstrations fully comply with U.S. law and whether advanced DoD sensors can legally be used in domestic CD operations when they are operated by U.S. military forces. In this report, the authors examine federal law and DoD policy to answer these questions. Some parts of U.S. law mandate information-sharing among federal departments and agencies for national security purposes and direct DoD to play a key role in domestic CD operations in support of U.S. law enforcement agencies, while other parts of the law place restrictions on when the U.S. military might participate in law enforcement operations. Reviewing relevant federal law and DoD policy, the authors conclude that there is no legal reason why a DoD sensor should be excluded from use in an interagency technology demonstration or in an actual CD operation as long as a valid request for support is made by an appropriate law enforcement official and so long as no personally identifiable or private information is collected. The authors recommend DoD policy on domestic CD operations be formally clarified and that an approval process be established for technology demonstrations with a CD nexus.

Find the full report at www.rand.org/pubs/research_reports/RR551

Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing

Brett Hemenway, William Welser IV, and Dave Baiocchi

RR-344-AF (2014)

Space debris—the man-made orbital junk that represents a collision risk to operational satellites—is a growing threat that will increasingly affect future space-related mission designs and operations. Since 2007, the number of orbiting debris objects has increased by over 40 percent as a result of the 2007 Chinese antisatellite weapon test and the Iridium/Cosmos collision in 2009. With this sudden increase in debris, there is a renewed interest in reducing future debris populations using political and technical means. The 2010 U.S. Space Policy makes several policy recommendations for addressing the space congestion problem. One of the policy's key suggestions instructs U.S. government agencies to promote the sharing of satellite positional data, as this can be used to predict (and avoid) potential collisions. This type of information is referred to as space situational awareness (SSA) data, and, traditionally, it has been treated as proprietary or sensitive by the organizations that keep track of it because it could be used to reveal potential satellite vulnerabilities. This document examines the feasibility of using modern cryptographic tools to improve SSA. Specifically, this document examines the applicability and feasibility of using cryptographically secure multiparty computation (MPC) protocols to securely compute the collision probability between two satellites. These calculations are known as conjunction analyses. MPC protocols currently exist in the cryptographic literature and would provide satellite operators with a means of computing conjunction analyses while maintaining the privacy of each operator's orbital information.

Find the full report at www.rand.org/pubs/research_reports/RR344

Additional References

Alkire, Brien, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Danescu, William Fry, D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie Riposo, Timothy Smith, and Alexander Stephenson, *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, Santa Monica, Calif.: RAND Corporation, RR-1330-AF, 2016. As of April 9, 2020: www.rand.org/pubs/research_reports/RR1330

Anton, Philip S., Megan McKernan, Ken Munson, James G. Kallimani, Alexis Levedahl, Irv Blickstein, Jeffrey A. Drezner, and Sydne Newberry, *Assessing Department of Defense Use of Data Analytics and Enabling Data Management to Improve Acquisition Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-3136-OSD, 2019. As of February 26, 2020: www.rand.org/pubs/research_reports/RR3136

Bodine-Baron, Elizabeth, Todd C. Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, Calif.: RAND Corporation, RR-1328-RC, 2016. As of April 9, 2020: www.rand.org/pubs/research_reports/RR1328

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018. As of February 25, 2020: www.rand.org/pubs/research_reports/RR2740

Connor, Kathryn, Ian P. Cook, Isaac R. Porche III, and Daniel Gonzales, *Cost Considerations in Cloud Computing*, Santa Monica, Calif.: RAND Corporation, PE-113-A, 2014. As of November 18, 2020: www.rand.org/pubs/perspectives/PE113

Costello, Katherine, *Russia's Use of Media and Information Operations in Turkey: Implications for the United States*, Santa Monica, Calif.: RAND Corporation, PE-278-A, 2018. As of February 25, 2020: www.rand.org/pubs/perspectives/PE278

Crane, Conrad, "The United States Needs an Information Warfare Command: A Historical Examination," *War on the Rocks*, June 14, 2019. As of February 26, 2020: https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/

Diresta, Renee, and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, Stanford, Calif.: Stanford Internet Observatory Cyber Policy Center, November 2019. As of November 20, 2020: https://cyber.fsi.stanford.edu/io/news/potemkin-pages-personas-blog

Dougherty, Christopher M., *Why America Needs a New Way of War*, Washington, D.C.: Center for a New American Security, June 2019. As of November 18, 2020: https://s3.amazonaws.com/files.cnas.org/CNAS+Report+-+ANAWOW+-+FINAL2.pdf

Galvan, David A., Brett Hemenway, William Welser IV, and Dave Baiocchi, *Satellite Anomalies: Benefits of a Centralized Anomaly Database and Methods for Securely Sharing Information Among Satellite Operators*, Santa Monica, Calif.: RAND Corporation, RR-560-DARPA, 2014. As of April 9, 2020: www.rand.org/pubs/research_reports/RR560

Gonzales, Daniel, Sarah Harting, Jason Mastbaum, and Carolyn Wong, *Improving Interagency Information Sharing Using Technology Demonstrations: The Legal Basis for Using New Sensor Technologies for Counterdrug Operations Along the U.S. Border*, Santa Monica, Calif.: RAND Corporation, RR-551-OSD, 2014. As of April 9, 2020: www.rand.org/pubs/research_reports/RR551

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018. As of February 25, 2020: www.rand.org/pubs/research_reports/RR2237

Helmus, Todd C., and Elizabeth Bodine-Baron, *Empowering ISIS Opponents on Twitter*, Santa Monica, Calif.: RAND Corporation, PE-227-RC, 2017. As of April 9, 2020: www.rand.org/pubs/perspectives/PE227

Hemenway, Brett, William Welser IV, and Dave Baiocchi, *Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing*, Santa Monica, Calif.: RAND Corporation, RR-344-AF, 2014. As of April 9, 2020: www.rand.org/pubs/research_reports/RR344

Hollywood, John S., Michael J. D. Vermeer, Dulani Woods, Sean E. Goodison, and Brian A. Jackson, *Using Social Media and Social Network Analysis in Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-2301-NIJ, 2018. As of February 25, 2020: www.rand.org/pubs/research_reports/RR2301

Hollywood, John S., and Zev Winkelman, *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?*, Santa Monica, Calif.: RAND Corporation, RR-645-NIJ, 2015. As of February 26, 2020: www.rand.org/pubs/research_reports/RR645

Jackson, Brian A., *How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts*, Santa Monica, Calif.: RAND Corporation, RR-380-OSD, 2014. As of February 26, 2020: www.rand.org/pubs/research_reports/RR380

Jackson, Brian A., Lane F. Burgette, Caroline Stevens, Claude Messan Setodji, Erinn Herberman, Stephanie Ann Kovalchik, Katie Mugg, Meagan Cahill, Jessica Hwang, and Joshua Lawrence Traub, *Knowing More, but Accomplishing What? Developing Approaches to Measure the Effects of Information-Sharing on Criminal Justice Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-2099-NIJ, 2017. As of April 9, 2020: www.rand.org/pubs/research_reports/RR2099

Jahedi, Salar, Jennie W. Wenger, and Douglas Yeung, *Searching for Information Online: Using Big Data to Identify the Concerns of Potential Army Recruits*, Santa Monica, Calif.: RAND Corporation, RR-1197-A, 2016. As of February 26, 2020: www.rand.org/pubs/research_reports/RR1197

Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington, D.C., January 2021, p. 104. As of February 25, 2020: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Knopp, Bradley, Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson, *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, RR-1582-DIA, 2016. As of February 26, 2020: www.rand.org/pubs/research_reports/RR1582

Koerner, Brendan I., "Inside the Cyberattack That Shocked the US Government," *Wired*, October 23, 2016. As of February 26, 2020: www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Lim, Nelson, Bruce R. Orvis, and Kimberly Curry Hall, *Leveraging Big Data Analytics to Improve Military Recruiting*, Santa Monica, Calif.: RAND Corporation, RR-2621-OSD, 2019. As of February 26, 2020: www.rand.org/pubs/research_reports/RR2621

Matthews, Miriam, Christopher Paul, David Schulker, and David Stebbins, *Frameworks for Assessing USEUCOM Efforts to Inform, Influence, and Persuade*, Santa Monica, Calif.: RAND Corporation, RR-2998-EUCOM, 2020. As of November 20, 2020: www.rand.org/pubs/research_reports/RR2998

Mazarr, Michael J., Ryan Michael Bauer, Abigail Casey, Sarah Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2714-OSD, 2019. As of February 26, 2020: www.rand.org/pubs/research_reports/RR2714

Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, Santa Monica, Calif.: RAND Corporation, RR-2713-OSD, 2019. As of April 9, 2020: www.rand.org/pubs/research_reports/RR2713

Marcellino, William, Krystyna Marcinek, Stephanie Pezard, and Miriam Matthews, *Detecting Malign or Subversive Information Efforts over Social Media: Scalable Analytics for Early Warning*, Santa Monica, Calif.: RAND Corporation, RR-4192-EUCOM, 2020. As of November 20, 2020: www.rand.org/pubs/research_reports/RR4192

Marcellino, William, Meagan L. Smith, Christopher Paul, and Lauren Skrabala, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, Santa Monica, Calif.: RAND Corporation, RR-1742-OSD, 2017. As of February 25, 2020: www.rand.org/pubs/research_reports/RR1742

McKernan, Megan, Nancy Young Moore, Kathryn Connor, Mary E. Chenoweth, Jeffrey A. Drezner, James Dryden, Clifford A. Grammich, Judith D. Mele, Walter T. Nelson, Rebeca Orrie, Douglas Shontz, and Anita Szafran, *Issues with Access to Acquisition Data and Information in the Department of Defense: Doing Data Right in Weapon System Acquisition*, Santa Monica, Calif.: RAND Corporation, RR-1534-OSD, 2017. As of February 26, 2020: www.rand.org/pubs/research_reports/RR1534

Merriam-Webster.com, "Information," webpage, undated. As of February 25, 2020: www.merriam-webster.com/dictionary/information

Muñoz, Arturo, and Erin Dick, *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness*, Santa Monica, Calif.: RAND Corporation, PE-128-OSD, 2015. As of February 26, 2020: www.rand.org/pubs/perspectives/PE128

Paul, Christopher, "Is It Time to Abandon the Term Information Operations?" *Strategy Bridge*, March 11, 2019.

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018. As of April 9, 2020: www.rand.org/pubs/research_reports/RR1925z1

Paul, Christopher, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2489-OSD, 2018. As of February 26, 2020: www.rand.org/pubs/research_reports/RR2489

Paul, Christopher, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of February 25, 2020: www.rand.org/pubs/perspectives/PE198

Paul, Christopher, Yuna Huh Wong, and Elizabeth M. Bartels, *Opportunities for Including the Information Environment in U.S. Marine Corps Wargames*, Santa Monica, Calif.: RAND Corporation, RR-2997-USMC, 2020. As of November 18, 2020: www.rand.org/pubs/research_reports/RR2997

Paul, Christopher, Jessica Yeats, Colin P. Clarke, and Miriam Matthews, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*, Santa Monica, Calif.: RAND Corporation, RR-809/1-OSD, 2015. As of February 26, 2020: www.rand.org/pubs/research_reports/RR809z1

Pomerleau, Mark, "Congress Wants to Up DoD's Game in the Information Environment," *C4ISRNet*, December 10, 2019. As of February 26, 2020: www.c4isrnet.com/information-warfare/2019/12/10/congress-wants-to-up-dods-game-in-the-information-environment/

Porche III, Isaac R., Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman, *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information*, Santa Monica, Calif.: RAND Corporation, RR-315-NAVY, 2014. As of November 18, 2020: www.rand.org/pubs/research_reports/RR315

Riposo, Jessie, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar, and Jerry M. Sollinger, *Issues with Access to Acquisition Data and Information in the Department of Defense*, Santa Monica, Calif.: RAND Corporation, RR-880/1-OSD, 2015. As of February 26, 2020: www.rand.org/pubs/research_reports/RR880z1

Robinson, Neil, Jon Freeman, Jan Gaspers, Veronika Horvath, Tess Hellgren, and Alex Hull, *Living Room Connected Devices: Opportunities, Security Challenges and Privacy Implications for Users and Industry*, Santa Monica, Calif.: RAND Corporation, RR-604-OFCOM, 2014. As of April 9, 2020: www.rand.org/pubs/research_reports/RR604

Ronfeldt, David, and John Arquilla, *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft*, Santa Monica, Calif.: RAND Corporation, PE-A237-1, 2020. As of November 20, 2020: www.rand.org/pubs/perspectives/PEA237-1

U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018. As of February 25, 2020: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017. As of May 21, 2020: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Williams, Heather J., and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Santa Monica, Calif.: RAND Corporation, RR-1964-OSD, 2018. As of February 26, 2020: www.rand.org/pubs/research_reports/RR1964

Yerukhimovich, Arkady, Rebecca Balebako, Anne Boustead, Robert K. Cunningham, William Welser IV, Richard Housley, Richard Shay, Chad Spensky, Karlyn D. Stanley, Jeffrey Stewart, Ari Trachtenberg, and Zev Winkelman, *Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices*, Santa Monica, Calif.: RAND Corporation, RR-1393-DARPA, 2016. As of April 9, 2020: www.rand.org/pubs/research_reports/RR1393

Young, William, and David Stebbins, *A Rapidly Changing Urban Environment: How Commercial Technologies Can Affect Military Intelligence Operations*, Santa Monica, Calif.: PE-181-OSD, 2016. As of February 26, 2020: www.rand.org/pubs/perspectives/PE181

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

Headquarters Campus
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

Washington, DC • Pittsburgh, PA • Boston, MA • Cambridge, UK • Brussels, BE • Canberra, AU

www.rand.org

CP-A614-4