Table of Contents

National security applications of social and behavioural science – reading

This week's reading is from a recent US study into ways in which social and behavioural science could support the work of the Intelligence Community.

There is a lot here, but some is optional. Please read in the following order:

- Two communities (pp 31 -47, particularly pp 36-45)
- Strengthening ties (pp 289 - 306)
- Capitalising on opportunities (pp 319-326)

- Optional: Summary of study (pp 1-13)

Questions we will be discussing in class:

- Do you agree with the areas of opportunity highlighted in this report? What is missing?
- What opportunities to incorporate social and behavioural science and/or to work with social and behavioural scientists exist in your own areas of work?
- What challenges might you face in seeking to take advantage of these opportunities?

Note: The entire report can be downloaded for free here: https://www.nap.edu/catalog/25335/a-decadal-survey-of-the-social-and-behavioral-sciences-a

Reference

National Academies of Sciences, Engineering, and Medicine 2019. *A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis.* Washington, DC: The National Academies Press. https://doi.org/10.17226/25335.

2

Two Communities

The Intelligence Community (IC) and the social and behavioral sciences (SBS) research community have had many opportunities to work jointly since the early 20th century, and several structures are currently in place to facilitate that collaboration (see Chapter 9 and Appendix A). Nonetheless, each of these communities has a distinct culture and has developed specialized ways of working. For readers not already deeply familiar with the way both academic researchers and IC analysts work, it may be useful to learn more about the contexts in which their work is carried out. This chapter provides a brief introduction to the two communities and offers some observations about similarities and differences in the challenges of research and analysis they face.

THE UNIVERSE OF INTELLIGENCE AND NATIONAL SECURITY

The United States devotes considerable resources to intelligence and national security (see Box 2-1). In 2017, the total spent on intelligence was $70.3 billion, of which $53.5 billion was for national intelligence (the remainder was for military intelligence) (Miles, 2016). This work is carried out by what is loosely known as the IC, defined by the Office of the Director of National Intelligence (ODNI) as "a federation of executive branch agencies and organizations that work separately and together to conduct

BOX 2-1
Definition of Intelligence

Intelligence is information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security. Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform official travelers of counterintelligence and security threats.

SOURCE: Excerpted from https://www.dni.gov/index.php/what-we-do/what-is-intelligence [January 2019].

intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States."[1]

The work of the 17 agencies that make up the IC[2] (see Box 2-2) is not readily understood by outside observers. Much of that work is classified, and those who perform it rely on complex procedures and traditions that have developed over decades. During the past few decades, the public and the academic community have sought greater understanding of how the national security infrastructure—which carries out a function widely recognized as critical—functions. Aspects of the agencies' work have become better understood, in part because of journalists' and scholars' pressure for access to both historical and current information, and in part as a result of the work of a growing number of academic researchers drawn from such fields as history, international studies, and political science who have focused on the study of intelligence gathering and assessment (Monaghan, 2009), contributing interdisciplinary understanding of the role and functioning of spy agencies, intelligence abuses, and other issues.[3]

[1]Available: https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf [January 2019].

[2]The terms "national security," "defense," "intelligence," and "Intelligence Community" are used somewhat informally to refer to related and sometimes overlapping functions associated with protecting the United States from domestic and external threats. In this report we focus on the work of intelligence analysts—those employed by the 17 IC agencies to analyze intelligence; when we refer to the IC, we mean that workforce and the agency leadership that oversees it.

[3]See, for example, the *Journal of Intelligence and National Security*, *Journal of National Security*, and *Journal of Global Security Issues*.

BOX 2-2
The 17 Entities That Make Up the Intelligence Community

Department of Defense Entities:

1. Defense Intelligence Agency
2. National Geospatial-Intelligence Agency
3. National Reconnaissance Office
4. National Security Agency
5. U.S. Air Force Intelligence
6. U.S. Army Intelligence
7. U.S. Marine Corps Intelligence
8. U.S. Navy Intelligence

Non–Defense Department Entities:

9. Office of the Director of National Intelligence
10. Central Intelligence Agency

Department of Energy

11. *Office of Intelligence and Counter-Intelligence*

Department of Justice

12. *Federal Bureau of Investigation's National Security Branch*
13. *Drug Enforcement Agency's Office of National Security Intelligence*

Department of Homeland Security

14. *Office of Intelligence and Analysis*
15. *U.S. Coast Guard Intelligence*

Department of State

16. *Bureau of Intelligence and Research*

Department of the Treasury

17. *Office of Intelligence and Analysis*

NOTE: Italics indicate the specific offices of the listed parent agencies that are part of the Intelligence Community.
SOURCE: Adapted from Miles (2016).

The focus of this report is on the work of the intelligence analyst, carried out in the IC context. In this section, we provide an overview of the primary functions of the agencies dedicated to protecting the nation's security, based on information made publicly available through official documents and websites produced by the IC agencies.

The Security Infrastructure

The government officials responsible for the nation's security rely on information collected by the IC. Each of the 17 IC agencies has a particular focus and mission, but together they provide support to decision makers (often referred to as "customers" or "clients" because it is they who act

on the intelligence provided) in the executive and legislative branches of government, law enforcement, and the military.

The National Security Act of 1947[4] launched the U.S. national security establishment. The changing nature of both foreign and domestic threats, as well as differing views about such issues as the purposes for which intelligence may be collected and used, the proper leadership and oversight for agencies involved in collecting it, and protections for U.S. citizens' privacy, has influenced numerous reorganizations of the IC in the course of the nation's history (Federation of American Scientists, 1996; Rosenwasser and Warner, 2017). As new agencies involved in collecting and analyzing intelligence have emerged, coordinating their work has become an increasing challenge. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[5] established ODNI to lead the IC, and charged it with synchronizing the collection, analysis, and counterintelligence carried out across the IC agencies (Office of the Director of National Intelligence, 2013).[6]

While the structure of the IC has evolved in response to the nation's changing needs, its overall responsibility has not changed: it is collectively responsible for identifying issues that need to be investigated, collecting and analyzing relevant information of many kinds, and conveying the information and analysis in a timely manner to those who need them while also keeping the information secure and complying with laws regarding its collection and handling.

Of the 17 IC agencies, all but 9 reside within the U.S. Department of Defense (DoD). While ODNI has a coordination function, it is also an agency itself, as is the Central Intelligence Agency (CIA).[7] Five departments of the executive branch have their own intelligence agencies as well: the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) under the Department of Justice and agencies under the Departments of Energy, Homeland Security, State, and Treasury (refer to Box 2-1).

The IC agencies are guided by "a multitude of laws, executive orders, policies, and directives," and their missions overlap to some extent (Federation of American Scientists, 1996). The entire IC is guided by Executive Order 12333 (as amended),[8] but each of the IC agencies also contains many offices, directorates, and other units, each with its own areas of authority, methods, and responsibilities. For example, the CIA integrates intelligence

[4]*National Security Act of 1947*, Public Law No. 80-253, 61 Stat. 495 (1947).

[5]*Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law No. 108-458, 118 Stat. 3638 (2004).

[6]For a detailed look at the history and culture of the agencies that make up the national security community, see George and Rishikof (2017).

[7]Available: https://www.dni.gov/index.php/what-we-do [January 2019].

[8]Exec. Order No. 12,333, 3 C.F.R. 200 (1981), reprinted in 50 U.S.C. § 401 app. at 44-51 (1982).

from all sources into a body of "national intelligence" that supports the development of foreign and domestic policy; it is also the principal collector of certain types of intelligence and has responsibility for covert action. The FBI's mission is to "protect the America people and uphold the Constitution of the United States," but it also has agents in other nations and collects intelligence of many sorts (Federal Bureau of Investigation, 2018). The Department of Homeland Security has an almost identical mission—to "safeguard the American people, our homeland, and our values"—although it focuses on threats to aviation and border security, the integrity of cyber networks, and violent extremism (U.S. Department of Homeland Security, 2018). The Defense Intelligence Agency (DIA) has a different focus: integration of intelligence collected by the various service branches into "defense intelligence" used to support the missions of U.S. military forces (Defense Intelligence Agency, 2018).

Types of Intelligence

There are many different types of intelligence that reflect the purposes for which they are collected. While no canonical definitions exist for these various types of intelligence, ODNI defines as the foundational intelligence mission of the IC the collection of the following:

- strategic intelligence—"to inform and enrich understanding of enduring national security issues";
- anticipatory intelligence—"to detect, identify, and warn of emerging issues and discontinuities"; and
- current operations—"to support ongoing actions and sensitive intelligence operations."[9]

Observers of intelligence work also commonly distinguish among strategic intelligence, used by "policymakers to make policy and military decisions at the national and international level" (Rosenbach and Peritz, 2009, p. 10); operational intelligence, used by "leaders to plan and accomplish strategic objectives within the operational area" (Rosenbach and Peritz, 2009, p. 10); and tactical intelligence, best known as the information provided to military leaders in the field to support them in planning and executing battles and engagements, helping them "accomplish immediate tactical objectives" (Rosenbach and Peritz, 2009, p. 10). As the ODNI definition indicates, strategic intelligence deals with long-range issues and needs related to the development of national strategy and policy. It is a primary source of insights into international situations, and supports the

[9]Available: https://www.dni.gov/index.php/what-we-do/what-is-intelligence [January 2019].

development of military plans and strategic operations (Clark, 2013; Miles, 2016). Operational intelligence concerns the capabilities and intentions of adversaries, and is used both in military contexts (e.g., to monitor events or support military campaigns) and in diplomatic contexts (e.g., to support negotiation of an arms reduction treaty). Law enforcement also may use operational intelligence to plan an operation, such as mass arrest of members of an organized crime syndicate (Clark, 2013; Miles, 2016). Tactical intelligence provides commanders with information regarding imminent threats to their forces and changes in the operational environment (Miles, 2016). Law enforcement uses tactical intelligence in a similar manner.

These categories of intelligence encompass a wide range of information needs and possible sources of information. It is important to note as well that intelligence includes more than information that is gathered through clandestine means or needs to be classified; it also includes many types of readily available information, and a key function of the analyst is to identify which information will be useful to the client. In developing strategic plans, for example, policy makers may need analyses of developments in a geographic area that are based on historical and political science research, as well as continuous monitoring of groups and trends, but that also reflect up-to-the-minute intelligence about fast-moving events. Decision makers may need support in anticipating immediate or longer-range threats or opportunities, in making sense of unexpected developments, or in responding to crises. The six basic types of raw information that make up most intelligence are described in Box 2-3. They are distinguished primarily by the methods used to collect the information, and multiple agencies may contribute to the collection of each type (Krizan, 1999; Office of the Director of National Intelligence, 2019; Rosenbach and Peritz, 2009).

The IC agency tasked with providing the intelligence and the client (i.e., user of the intelligence) must work together: the analyst must understand the client's intelligence need to identify and efficiently synthesize the information that will meet that need. As discussed in greater detail in Chapter 4, the analyst's responsibility is to provide information that is as complete and accurate as possible, but often in an extremely tight timeframe. Frequently, the client's need is both complex and urgent: the questions requiring answers may require both deep understanding of social, cultural, and historical trends and the integration of complex technologically generated information, all in the context of fast-moving developments in which lives may hang on a policy maker's decision.

THE SOCIAL AND BEHAVIORAL SCIENCES

The set of academic disciplines generally referred to as the social and behavioral sciences (SBS) is large and diverse. Researchers in these fields use

BOX 2-3
Types of Intelligence Information[a]

1. **SIGINT—**Signals intelligence is derived from signal intercepts comprising—however transmitted, and either individually or in combination—all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). The National Security Agency (NSA) is responsible for collecting, processing, and reporting SIGINT. The National SIGINT Committee within NSA advises the director, NSA, and the director of national intelligence (DNI) on SIGINT policy issues and manages the SIGINT requirements system.
2. **IMINT—**Imagery intelligence includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, and electro-optics. The National Geospatial-Intelligence Agency (NGA) is the manager for all IMINT activities, both classified and unclassified, within the government, including requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.
3. **MASINT—**Measurement and signature intelligence is technically derived intelligence data other than SIGINT and IMINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. Its collection employs a broad group of disciplines, including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. Examples might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. The Directorate for MASINT and Technical Collection (DT), a component of the Defense Intelligence Agency, is the focal point for all national and Department of Defense MASINT matters.
4. **HUMINT—**Human intelligence is derived from human sources. To the public, HUMINT remains synonymous with espionage and clandestine activities; however, most HUMINT collection is performed by overt collectors such as strategic debriefers and military attaches. HUMINT represents the oldest method for collecting information, and until the technical revolution of the mid- to late 20th century, it was the primary source of intelligence.
5. **OSINT—**Open-source intelligence is publicly available information appearing in print or electronic form, including radio; television; newspapers; journals; the Internet; commercial databases; and videos, graphics, and drawings. While OSINT collection responsibilities are broadly distributed throughout the IC, the major collectors are the DNI's Open Source Center (OSC) and the National Air and Space Intelligence Center (NASIC).
6. **GEOINT—**Geospatial intelligence is the product of the analysis and visual representation of security-related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.

[a]For more information on the contributions on these types of intelligence and how they are collected, see, e.g., Krizan (1999), Office of the Director of National Intelligence (2019), and Rosenbach and Peritz (2009).

SOURCE: Adapted from Krizan (1999), Office of the Director of National Intelligence (2019), and Rosenbach and Peritz (2009).

a wide range of scientific methods, research strategies, and tools and rely on diverse theoretical approaches,[10] but what they share is "their analytic focus on the behavior, attitudes, beliefs, and practices of people and their organizations, communities, and institutions" (National Research Council, 2012, p. 10). SBS researchers inquire into people and what they do from many different stances and ask a wide variety of questions about individuals, groups, communities, societies, and nations. They may examine, for example, individual mental processes that guide behavior, ways in which cultural practices and attitudes are shared and evolve across generations, or how water shortages are influencing political developments in a particular region. Within each SBS discipline, moreover, there are multiple subspecialties that have developed their own research approaches and methodologies. This is a large research community: by one estimate it encompasses 35,490 social scientists in the United States alone, and that number does not include researchers employed outside of academic institutions (U.S. Bureau of Labor Statistics, 2018). Research collaboration and sharing of knowledge across international borders are commonplace in SBS disciplines as well; U.S. researchers expand their knowledge through international journals and academic conferences.

While it is not simple to develop a comprehensive list of SBS fields, they include areas as diverse as demography and social statistics, sociology, economics, linguistics, social anthropology, international relations, and psychology. Most—though not all—of these fields have applications important for national security. The challenges and risks discussed in this report reflect the importance of analyses that, for example, reveal implications of the aging of populations in certain countries, support forecasts of political crises, or indicate shifts in the narratives of extremist groups that provide indicators of objectives or targets.

Researchers across SBS fields use many different research approaches, including varieties of experimental and observational studies, evaluation, meta-analysis, and qualitative and mixed-methods research.[11] As discussed below, significant advances have recently been made possible by expanded computing power, increased capacity for work with large-scale datasets, and improved methods of analysis (National Research Council, 2012). A comprehensive grounding in the methods and approaches used across the

[10]This report addresses many aspects of SBS research. The term "research tools" is used to refer to specific means of collecting data, including both traditional means, such as questionnaires or survey instruments, and such technology-supported tools as software for use with large-scale datasets. The terms "research approach" and "theoretical approach" are used to refer to the researcher's theoretically based ideas about how to apply tools and methodology to answer a defined question.

[11]See National Research Council (2012) for an overview of research methods used in the SBS and their assets and limitations.

SBS is beyond the scope of this report, but before turning to key technological developments, we note three general trends that apply across SBS fields.

One important trend is an increase in work that cuts across disciplines, in some cases yielding new hybrid disciplines (transdisciplinary research) (Scott et al., 2015). Integrating research methods and types of data from different disciplines, including many of the physical and life sciences, has proven critical for satisfactorily investigating complex problems. For example, researchers interested in environmental sustainability have recognized that to develop a complete picture, it is necessary to combine understanding of such areas as human cognition, risk perception, economic behavior, and problem solving and decision making with understanding of climate change and its impacts on weather and infrastructure (see, e.g., Tainter et al., 2015). Interdisciplinary work is particularly important in the context of the technological advances discussed below.

Also of note—and an important intellectual backdrop for much of the research discussed in this report—is a significant evolution in thinking that has grown out of work involving not only such SBS fields as neuro- and cognitive psychology, social psychology, and sociology but also physical and life science disciplines, including neuroscience and genetics. Building on work by Bronfenbrenner and others (e.g., Bronfenbrenner, 1977, 1994) that elaborated on how the individual is influenced by family, community, and the broader social context, researchers have developed a much more sophisticated picture of these interactions.[12] Emerging work has demonstrated the dynamic interplay between human development and the environment—from the genetic and epigenetic levels to the broadest sociocultural level. Insights about the importance of culture and environment have profoundly influenced the study of many aspects of the human experience, including learning and development (see NASEM, 2018) and the factors that influence mental and behavioral disorders in young people (see NASEM, forthcoming). This rapidly developing area of study has clear implications for security-related topics, from the growth of extremist ideology in an individual to the influences that shape the beliefs and norms of a particular group or society. Application of these emerging ideas in the context of national security concerns is a promising frontier for further research.

A third trend that cuts across SBS fields is growing understanding that a significant majority of SBS research has relied on information collected within cultures that are Western, educated, industrial, rich, and democratic (WEIRD). Conclusions drawn from research conducted with samples that are limited in this way cannot readily be applied beyond the context in which the data were collected; this is known as the WEIRD problem (see, e.g., Henrich et al., 2010; Nielsen et al., 2017; see also the

[12]See NASEM (2018, Chapter 2) for a detailed discussion of these developments.

discussion of study populations in NASEM, 2018). Researchers across numerous fields have become increasingly circumspect about considering these characteristics in the design of studies and the analysis and reporting of results. This issue has particular relevance for the IC, not least because the IC is concerned with understanding the behavior and motivations of people and societies around the globe.

SHARED CHALLENGES AND DIVERSE DEMANDS

The accuracy and validity of research are of paramount importance for both the SBS researchers whose calling is to produce it and the intelligence analysts who rely on this and other research while also engaging in many forms of research in their own work. Moreover, understanding human behavior is, in a sense, the primary objective for each of these professional communities, and they draw on many of the same resources in their quests for that understanding. At the same time, however, very different pressures, constraints, and cultures have shaped these two professions. A brief look at an emerging phenomenon—big data—that has had a significant impact on both SBS research and intelligence analysis highlights the overlap between these two endeavors; we also look briefly at interdisciplinary collaborations and at key differences between the two communities.

More Data and More Ways to Analyze Them

The digitization of society has resulted in an exponential increase in the amount of data available to analyze, and has made access to new sorts of data easy and widespread—a phenomenon loosely referred to as "big data."[13] While there is no one best definition of the term "big data," it is generally used to refer to extremely large sets of digital data that cannot be digested without advanced analytic techniques. This development has had a profound influence on the kinds of work that can be done by both SBS researchers and the IC. It has led to increased interdisciplinary collaboration (see below), increased use of mixed methods, increased reliance on computational techniques and models, and increased reliance on online environments and publicly available data for research (Scott et al., 2015).

Digital data fall into two categories. Most broadly, virtually all existing forms of data are now routinely archived digitally. Historical information that would be of interest to the IC and was originally stored in analog form is being converted to digital form through scanning and optical character recognition. These data are stored in digital repositories accessible through

[13]For discussion of the analysis of large-scale data and mathematical analysis in an intelligence and defense context, see NASEM (2017a).

websites. A second, more rapidly growing category of digital data is information being generated continuously on digital platforms supported by Internet and web protocols. These data include the content—text, graphics, audio, and video—resulting from actions, interactions, and transactions that occur in digital space. In addition to this content, digital trace data provide "metadata" about, for instance, who interacts with whom, about what, and at what time.

All of these data offer unprecedented opportunities for both scholarly researchers and IC analysts. Beginning approximately a decade ago, both groups began to encounter exponentially increased volumes of data potentially relevant to their work, although much of the newer data is what statisticians term "noisy" (data whose significance is difficult or impossible to discern). This relatively new data glut has precipitated considerable progress in descriptive, predictive, and prescriptive analytic techniques as researchers have pursued ways to use newly available types of data:

- **Descriptive** analytic techniques are means of summarizing large tracts of data to discern patterns, often using exploratory data analyses. These techniques can be used, for instance, to detect a significant and abrupt growth in messaging within an adversarial social network.
- **Predictive** analytic techniques are means of discerning associations among variables, with the goal of predicting certain variables (e.g., civil unrest) based on their association with others (e.g., use of certain terms in social media chatter). Machine learning techniques are valuable for this sort of analysis: computers are "trained" with known data (e.g., available historical data about the variable of interest) to recognize the sorts of patterns in which the analyst is interested, and the resulting algorithms are used to make predictions about the variable of interest (NASEM, 2018).
- **Prescriptive** analytic techniques are particularly useful for identifying which variables can be manipulated to result in a desired change in the variable of interest. Here, recent advances in what are called optimization techniques can leverage insights from machine learning models to go beyond predicting what might happen to offering insights on what to manipulate to bring about a desired outcome. A helpful, although not entirely accurate, analogy can be found in climate science. In that field, descriptive analytics indicate the current weather conditions, while predictive analytics indicate the forecast. Prescriptive analytics might result in recommending the use of cloud seeding to trigger precipitation.

Interdisciplinary Collaborations

Advances in large-scale data collection and computational analytic techniques, as well as the continuing growth of computer power, have opened up promising new frontiers in SBS research (National Research Council, 2012). Large-scale datasets—including social media, events data, and geographic information system (GIS) data—are sources of information that analysts and policy makers can use to better monitor and understand global events in real time and at a finer granularity than was previously possible. Advances in machine learning, robust optimization, computer-assisted content analysis, social network analysis, agent-based modeling, and other emerging computational approaches are facilitating the generation of reliable and robust SBS insights using big data.

Machine learning tools such as Random Forest—an algorithm used for decision making and classification (see Breiman and Cutler, n.d.)—for example, have the potential to provide more accurate predictions of rare events, such as the outbreak of civil war, relative to traditional statistical methods (Muchlinski et al., 2016). Combining automated textual analysis and social network analysis, researchers have shown that it is possible to "analyze hacker chats and other data faster and more efficiently than had previously been possible," enabling them to identify hackers' intentions (NASEM, 2017b, p. 17). This work may improve forecasts of hacker threats (NASEM, 2017b). And recent research at the intersection of cognitive and computer science is generating new visualization tools that facilitate human exploration and understanding of the complex, multiscalar phenomena that are the subjects of computational social science (National Science Foundation, 2011).

Research at these new frontiers is often interdisciplinary, drawing on multiple methodological, theoretical, and empirical approaches. This is the case because the intellectual advances in these areas are most likely to occur at the nexus of advances in data science, computer science, and SBS research. Traditionally, SBS researchers have relied most heavily on theory-driven approaches that are either deductive (hypotheses derived from a priori theories) or inductive (theories inferred from data, sometimes referred to as "grounded theory"). In contrast, data science and computer scientists rely on data-driven approaches often focused primarily on prediction, even at the cost of theoretical explanation or understanding (Anderson, 2008). This artificial and unhelpful methodological divide can be transcended by interdisciplinary approaches that generate insights by iterating between theory-driven and data-driven approaches. The result has been renewed interest in what social scientists characterize as the abductive approach, to distinguish it from the deductive or inductive approach (Haig, 2005).

Indeed, recent assessments of the state and future of SBS research have focused on the advantages of interdisciplinary work in this area. The National Institutes of Health's Office of Behavioral and Social Research has highlighted the promise that interdisciplinary research exploiting new technologies and advances in data analytics holds for SBS knowledge (National Institutes of Health, 2017). And as emphasized by the National Science Foundation's *Rebuilding the Mosaic* report, which is based on a synthesis of more than 200 white papers from the SBS research community, the future of SBS research is "interdisciplinary, data-intensive, and collaborative" (National Science Foundation, 2011).

Another development is a recent move to thinking in terms of "broad" data, which offers researchers the unprecedented ability to fuse diverse sources of data, yielding information that is much more valuable than an undifferentiated stream of unstructured data. An example is the juxtaposition of neuroimaging and behavioral data on humans. This juxtaposition has demonstrated the potential for new theoretical advances in predicting, for instance, the efficacy of strategies designed to influence individuals' attitudes and behaviors based on activation of specific areas in the brain (Estrada et al., 2017). Another promising avenue has been the use of physical activity data on team members collected from wearable devices to offer new insights into team performance through real-time assessment of cognitive functioning (Kim et al., 2012; Pentland, 2012).

Cognitive neuroscience and related technologies are expected to continue to converge with and in some respects transform SBS research, drawing on advances in psychopharmacology, functional neuroimaging, and computational biology, among other fields. Models of psychological states and intentions are being drawn from increasingly sophisticated neurophysiological assessment technology. Noninvasive functional brain imaging technologies have been progressing rapidly (National Research Council, 2008), and may be applied to measurements of neural degeneration related to cognitive function and assessments of readiness for complex tasks.

These examples illustrate the significant potential of big data and related developments for both SBS researchers and intelligence analysts, but also highlight challenges. The scale of the available information continues to grow exponentially, and the pace of cyber-based developments also demands much faster responses. The Internet has often been described as the "wild west" because it is largely unregulated, although recent efforts to undermine democratic processes and other security threats are leading to an examination of possibilities for policing aspects of this realm. In any case, the openness and rapid pace of change characteristic of the Internet pose challenges for the IC and for researchers who hope to study the data it yields.

Diverse Cultures, Audiences, and Demands

Although challenges and opportunities presented by big data highlight possibilities that can benefit both the SBS research community and the IC, they also point to significant differences that have implications for the work the two communities do together. Many of these differences stem from the fundamentally different purposes of the researcher and the analyst. The researcher's basic purpose is to add to the sum of human knowledge using the methods of scholarship, including forming a hypothesis based on data collected, testing that hypothesis, analyzing the results, and drawing inferences based on the evidence obtained. Researchers are trained to use the methods honed within their specialty, and to apply and contribute to theoretical models designed to explain observable phenomena. They are encouraged to pursue questions because those questions are interesting and unanswered, even if the practical application of the answers is not immediately apparent. Although resource limitations—and the imperative to produce regular publications—are natural constraints, researchers generally feel relatively little pressure to produce results within a given timeframe.

Analysts, by contrast, are focused on objectives related to national security and foreign policy. As discussed in Chapter 4, they may have a range of specific assignments, which may require them to seek deep understanding of a region, historical trends, and other more general knowledge quite similar to that sought by academic researchers. But their attention does not waver from the potential application of that knowledge to security concerns: answering policy makers' questions about the world and alerting them to possible risks and opportunities. Typically, this means providing analysis that is a best guess based on the information available at the time. Researchers have the luxury of time to complete a systematic process of collecting and analyzing information and testing their conclusions, whereas analysts must often provide rapid-fire, definitive answers in urgent circumstances.

The academic researcher also generally has greater latitude than the analyst to plan a systematic approach to the collection of evidence. Few research projects afford the opportunity to collect all the data that could be of value, but means of addressing limitations can be part of the research design. Analysts, by contrast, must generally rely on data that are acquired opportunistically and are therefore not representative, unbiased samples. Bias and questions about representativeness also affect SBS research—and researchers, too, may take advantage of available data—but the data available to analysts may also be compromised by the efforts of adversaries to disguise the data or otherwise deceive, which adds a layer of questions about validity that do not affect most academic research.

Curiosity and educated guesswork likely play an important role in both academic research and intelligence analysis,[14] but a researcher is ultimately judged by his or her peers on the basis of the documented methods used in the research and the extent to which the work is substantiated by that of others. The analyst, on the other hand, is judged in practice primarily by the extent to which he or she has provided valuable information and answers to the decision makers who rely on that information.[15] The researcher's conclusions may be described in an article or book dozens or hundreds of pages long, and filled with contextual information and detailed discussion of how conclusions are supported. The analyst's results, by contrast, may be presented in a very brief text or PowerPoint presentation, or some other format, as needed by a client who must digest the results quickly and has very limited time for subtleties related to multiple alternatives or other complexities.

It is perhaps natural, then, that tensions have sometimes arisen when these two communities have collaborated, as discussed in Chapter 9. But it is also clear that the two share important interests and methods.

REFERENCES

Anderson, C. (2008). The end of theory: The data deluge makes the scientific method obsolete. *WIRED*, June 23. Available: https://www.wired.com/2008/06/pb-theory [November 2018].

Breiman, L., and Cutler, A. (n.d.). *Random Forests*. Available: https://www.stat.berkeley.edu/~breiman/RandomForests/cc_home.htm#workings theory [November 2018].

Bronfenbrenner, U. (1977). Toward an experimental ecology of human development. *American Psychologist, 32*(7), 513–531.

Bronfenbrenner, U. (1994). Ecological models of human development. In *International Encyclopedia of Education* (2nd ed., Vol. 3). Oxford, UK: Elsevier.

Clark, R. (2013). *Intelligence Collection*. Washington, DC: CQ Press.

Defense Intelligence Agency. (2018). *Office of Intelligence and Analysis Mission*. Available: https://www.dhs.gov/office-intelligence-and-analysis-mission [November 2018].

Estrada, M., Schultz, P.W., Silva-Send, N., and Boudrias, M.A. (2017). The role of social influences on pro-environment behaviors in the San Diego region. *Journal of Urban Health, 94*(2), 170–179.

Federal Bureau of Investigation. (2018). *Mission & Priorities*. Available: https://www.fbi.gov/about/mission [November 2018].

Federation of American Scientists. (1996). *An Overview of the Intelligence Community*. Available: https://fas.org/irp/offdocs/int023.html [November 2018].

George, R., and Rishikof, H. (2017). *The National Security Enterprise: Navigating the Labyrinth*. Washington, DC: Georgetown University Press.

[14]For discussion of the development of expertise and how it shapes an individual's capacity to integrate new information and recognize significant patterns and anomalies, see NASEM (2018); National Research Council (2000).

[15]There are analytic standards for the IC; see https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf [January 2019].

Haig, B.D. (2005). An abductive theory of scientific method. *Psychological Methods, 10*(4), 371–388.

Henrich, J., Heine, S.J., and Norenzayan, A. (2010). The weirdest people in the world? *Behavioral and Brain Sciences*, *33*(2-3), 61–135. doi:10.1017/S0140525X0999152X.

Kim, T., McFee, E., Olguin, D.O., Waber, B., and Pentland, A. (2012). Sociometric badges: Using sensor technology to capture new forms of collaboration. *Journal of Organizational Behavior, 33*(3), 412–427.

Krizan, L. (1999). *Intelligence Essentials for Everyone*. Washington, DC: Joint Military Intelligence College. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a476726.pdf [November 2018].

Miles, A.D. (2016). *Intelligence Community Programs, Management, and Enduring Issues*. Washington, DC: Congressional Research Service. Available: https://fas.org/sgp/crs/intel/R44681.pdf [November 2018].

Monaghan P. (2009). Intelligence studies. *The Chronical of Higher Education*, March 20. Available: https://www.chronicle.com/article/Intelligence-Studies/33353 [February 2019].

Muchlinski, D., Siroky, D., He, J., and Kocher, M. (2016). Comparing random forest with logistic regression for predicting class-imbalanced civil war onset data. *Political Analysis, 24*(1), 87–103.

National Academies of Sciences, Engineering, and Medicine (NASEM). (2017a). *Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions*. Washington, DC: The National Academies Press. doi:10.17226/23670.

NASEM. (2017b). *The Value of Social, Behavioral, and Economic Sciences to National Priorities: A Report for the National Science Foundation*. Washington, DC: The National Academies Press. doi:10.17226/24790.

NASEM. (2018). *How People Learn II: Learners, Contexts, and Cultures*. Washington, DC: The National Academies Press. doi:10.17226/24783.

NASEM. (forthcoming). Report of the Committee on Fostering Healthy Mental, Emotional, and Behavioral Development Among Children and Youth; see http://sites.nationalacademies.org/dbasse/bcyf/meb-health-promotion/index.htm.

National Academy of Sciences. (2018). *The Frontiers of Machine Learning: 2017 Raymond and Beverly Sackler U.S.–U.K. Scientific Forum*. Washington, DC: The National Academies Press. doi:10.17226/25021.

National Institutes of Health. (2017). *The Office of Behavioral and Social Sciences Research Strategic Plan 2017–2021*. Available: https://obssr.od.nih.gov/wp-content/uploads/2016/12/OBSSRSP-2017-2021.pdf [May 2017].

National Research Council. (2000). *How People Learn: Brain, Mind, Experience, and School: Expanded Edition*. Washington, DC: National Academy Press.

National Research Council. (2008). *Emerging Cognitive Neuroscience and Related Technologies*. Washington, DC: National Academy Press.

National Research Council. (2012). *Using Science as Evidence in Public Policy*. Committee on the Use of Social Science Knowledge in Public Policy. K. Prewitt, T.A. Schwandt, and M.L. Straf (Eds.). Division of Behavioral and Social Sciences and Education. Washington, DC: The National Academies Press.

National Science Foundation. (2011). *Rebuilding the Mosaic: Fostering Research in the Social, Behavioral, and Economic Sciences at the National Science Foundation in the Next Decade*. Arlington, VA: National Science Foundation. Available: https://www.nsf.gov/pubs/2011/nsf11086/nsf11086.pdf [November 2018].

Nielsen, M., Haun, D., Kärtner, J., and Legare, C.H. (2017). The persistent sampling bias in developmental psychology: A call to action. *Journal of Experimental Child Psychology*, *162*, 31–38. doi:10.1016/j.jecp.2017.04.017.

Office of the Director of National Intelligence. (2013). *U.S. National Intelligence: An Overview*. Available: https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf [November 2018].

Office of the Director of National Intelligence. (2019). *What Is Intelligence?* Available: https://www.dni.gov/index.php/what-we-do/what-is-intelligence [May 2019].

Pentland, A. (2012). The new science of building great teams. *Harvard Business Review*, April. Available: https://hbr.org/2012/04/the-new-science-of-building-great-teams [November 2018].

Rosenbach, E., and Peritz, A. (2009). *Confrontation or Collaboration? Congress and the Intelligence Community*. Cambridge, MA: Harvard University, Belfer Center for Science and International Affairs. Available: https://www.belfercenter.org/sites/default/files/legacy/files/energy-security.pdf [November 2018].

Rosenwasser, J., and Warner, M. (2017). History of the interagency process for foreign relations in the United States: Murphy's Law? In R. George and H. Rishikof (Eds.), *The National Security Enterprise: Navigating the Labyrinth* (2nd ed.) (pp. 13–31). Washington, DC: Georgetown University Press.

Scott, R.A., Buchmann, M.C., and Kosslyn, S.M. (2015). *Emerging Trends in the Social and Behavioral Sciences*. Hoboken, NJ: John Wiley & Sons. doi:10.1002/9781118900772.

Tainter, J.A., Taylor, T.G., Brain, R.G., and Lobo, J. (2015). *Sustainability.* Available: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118900772.etrds0326 [November 2018].

U.S. Bureau of Labor Statistics. (2018). *Occupational Employment and Wages, May 2017: 193099 Social Scientists and Related Workers, All Other*. Available: https://www.bls.gov/oes/current/oes193099.htm [November 2018].

U.S. Department of Homeland Security. (2018). *Office of Intelligence and Analysis Mission.* Available: https://www.dhs.gov/office-intelligence-and-analysis-mission [November 2018].

9

Strengthening Ties Between the Two Communities

An important part of this committee's charge was to propose ways to "facilitate productive interchange between the security community and the external social science research community" (refer to Box 1-1 in Chapter 1). In this chapter, we offer reflections on how these ties can be strengthened. We begin with reflections on what we learned about the relationship between these two communities from the process of conducting this decadal survey, and then explore past collaborations between the two communities, drawing lessons from both successful and less-successful experiences and offering our conclusions about ways to strengthen these ties.

LESSONS FROM CONDUCTING THE DECADAL SURVEY

The committee was asked to reflect on the process of conducting this decadal survey and identify insights and practices that could be useful for any future such studies in social and behavioral sciences (SBS) fields. As noted in Chapter 1, this study marked the first time the National Academies of Sciences, Engineering, and Medicine's decadal process was applied to SBS fields. The decadal process was chosen because the Office of the Director of National Intelligence (ODNI) recognized the need for a comprehensive look across this research landscape: the process offered a way to address the urgency of integrating SBS research into intelligence analysis while also opening the door to a wide array of ideas. Our observations about this process may bear on planning for any future decadal studies in this universe but may also help ODNI to continue capitalizing on SBS research in a systematic and continuous way, apart from any future decadal surveys.

Challenges and Benefits of a Broad Charge

The committee's charge did not identify a precise objective to be met within 10 years, akin to the development of a space telescope. Rather, it directed us to look for opportunities that would "contribute to the IC's analytic responsibilities," a task that by its nature is ongoing, not one that might be complete at the end of 10 years. The breadth of this charge, which required us to look across a very wide research landscape, initially appeared to be the greatest challenge, but it turned out to have significant advantages.

It was clear from the start that the processes used in prior decadal surveys would be valuable but not easy to apply to this committee's work.[1] In particular, we recognized that, while surveying the research community for ideas was a key element of the process for this study, there was no practical way to survey such a broad community systematically. Indeed, although there is in a sense a community of SBS researchers—in that researchers in these fields share many common interests—SBS is by no means a single discipline. No institution or entity links all members of this set of disciplines; rather, the various SBS disciplines form an abstract community that encompasses a wide range of theories and methods. Further, the breadth of our charge and the importance of representing such a diverse array of work had a cost in terms of the level of depth with which we could explore particular research areas. The product of our deliberations, then, certainly is not exhaustive, and it would be impossible to forecast precisely which areas of research across all SBS fields will make the most important contributions to the IC in the coming decade.

Despite these constraints, however, there were distinct benefits to casting a wide net in seeking intersections between the needs of the IC and the available SBS research. One benefit was that, because a multidisciplinary approach was necessary, our work was not driven by the perspectives of a single discipline, and we had no preconceptions about where to look for relevant work. The process we developed to pursue understanding of the needs of the IC and merge that understanding with input on potentially relevant research exposed us to new ideas while also supporting some of our hypotheses.

[1]For example, prior decadal committees relied on the work of subpanels, designated from the start of the project to gather information in particular relevant disciplines. This approach was not practicable for our decadal study because we could not assume that a particular set of individual disciplines would have the most important contributions to make to fulfill our charge. See Chapter 1 and Appendix B for description of the process used for this study.

Challenges in Integrating Social and Behavioral Sciences and Other Research

Although the committee's charge was to examine SBS research, exploiting most of the opportunities identified in this report will depend on integrating research from SBS fields as disparate as neuroscience, engineering, and computer science. There are always challenges when researchers from different fields work together. Researchers from different domains may each sometimes view their counterparts as naïve, but here we focus on some errors that might occur when technically based research is conducted without the benefit of deep SBS knowledge.

One potential problem is rediscovery, or the reinvention of wheels. For example, early roboticists interested in the coordination of groups of agents "discovered" a finding already well established by organizational science—that teams adapt more rapidly than do hierarchies (Bersin, 2017). Of greater concern are cases in which researchers unaware of well-established findings make significant errors. An example is when claims about networks based on mathematical analysis (Barabási and Bonabeau, 2003) contradicted earlier work in sociology and demography (Heathcote et al., 2000; Jones and Handcock, 2003) and were later disproved (Broido and Clauset, 2018). Such errors can be serious. For instance, when artificial intelligence (AI) techniques not based in results of computational models driven by SBS theory are used in ways that have concrete impacts for individuals, the result can be unintended discrimination or other harms (Hauch et al., 2015; Siegel, 2018).

SBS researchers and engineers, computer scientists, and physicists take different approaches even when addressing the same phenomena (Borgatti et al., 2009), and the benefit of integrating SBS methods and findings has been noted in such realms as health care delivery (Burger, 2017) and the marketing of technology (Brookey, 2007; Grindley, 1990). More generally, technological developments occur in a social and economic context, and SBS research is essential to understanding technology's potential applications and benefits, risks, and long-term effects (Smith and Stirling, 2007). The industrial revolution was not driven by improvements in manufacturing and engineering alone; SBS research was needed to support the development of applications of these advances (Porter, 1986). As discussed throughout this report, SBS perspectives are essential to the development of sound research and applications involving sophisticated technology, and direct collaboration across SBS and technological fields is necessary for that to happen.

Obstacles to Collaboration Between Researchers and the Intelligence Community

Adapting the decadal process to a new context also required that the committee simultaneously conduct this study and continuously take stock of the effectiveness of the study process. Doing so allowed us to see first-hand some of the obstacles to integration and collaboration between the two communities on which we were focusing. One such obstacle is that even within the IC, and in the context of the numerous mechanisms it already has in place for drawing specifically on SBS research, there appears to be less coordination between the two than would be optimal. Existing IC entities were developed to pursue particular missions, not necessarily with the goal of advancing the integration of SBS knowledge. This reality, along with the need to keep some projects or information classified, is likely to work against coordination of these communities, to say nothing of funding and political considerations that were beyond our purview.

Another obstacle to integration is that awareness of potential applications of research to IC needs is highly uneven across relevant SBS fields. It is notable, for example, that this report contains little discussion of developments in such fields as political science and international relations. These fields make extremely important contributions to national security, and have done so for decades. Yet there was little need to address them here because for the most part, scholars in these fields are highly attuned to security issues, and the IC is highly attuned to their findings. Methodological and technological breakthroughs of which the IC may not be fully aware seemed far more likely in other areas of the SBS terrain.

Applying the decadal survey process to the IC context had another significant benefit. The committee cast the widest possible net in seeking white papers and other input from the SBS community (refer to Chapter 1 and Appendix B). The results, while valuable and intriguing, also clearly demonstrate that there is a long way to go in building awareness within the SBS research community of the potential application of its work to national security. However, our iterative process did reveal elements that would likely have emerged even if a different, parallel set of committee members had embarked on this study and devised a different method for applying the decadal survey process in the IC context. Without a doubt, for example, any attempt to fulfill our charge would highlight the importance of learning more about human–machine interactions. Likewise, emerging research in data science has many potential applications to national security work that would surely be included in any report such as this in some form. It is similarly difficult to imagine that the critical importance of integrating insights about human behavior and group functioning into the pursuit of cybersecurity would not have been recognized.

Finally, an issue that was a key challenge for this committee may be relevant to any future efforts to cull information from this broad research landscape. We struggled to find the best way to take stock of the diverse knowledge and expertise brought by the 16 committee members, and to find an optimal way to take advantage of our own knowledge base while also extending our reach widely in areas not well known to any of us. Our own knowledge base was a valuable foundation, but it was also limited, as were our resources for supplementing it. The rapid project schedule required us to quickly assess promising areas in order to make decisions about how to use our six workshops and other information-gathering strategies; there was no established process on which we could rely for this purpose. This procedural challenge mirrors a challenge faced by the IC: to systematically utilize an ever-expanding base of foundational SBS research while also identifying new work in unexpected areas that may prove equally valuable.

BUILDING ON PAST COLLABORATIONS

As noted in the overview of the SBS community and the IC in Chapter 2, the objectives and perspectives of these two communities are not always aligned, but the two have always had much to learn from one another. The relevance of SBS research to national security challenges has been apparent to both communities at least since researchers first worked with the U.S. military during World War I.[2] The first division of the National Academy of Sciences devoted to SBS research, the Division of Anthropology and Psychology, formed committees to explore military issues as early as 1919. Collaborations between the security and SBS communities began to play a critical and sustained role in military operations, and to expand to intelligence issues beyond military concerns, once the United States became involved in World War II. Since then, research partnerships between the two communities have generated important scientific insights and provided valuable support for intelligence and security activities, although the relationship has not always been smooth.

[2]In 1916, the leadership of the National Academy of Sciences formally "place[d] itself at the disposal of the Government for any services within its scope." This involvement led directly to the establishment of the National Research Council, the operating arm of the Academy, which would "advise the nation on matters of science and engineering." For more information about this history, see https://sites.nationalacademies.org/PGA/PGA_180900 [November 2018] and http://www.nasonline.org/about-nas/history/archives/milestones-in-NAS-history/organization-of-the-nrc.htm [November 2018]. The institution formally changed its name to the National Academies of Sciences, Engineering, and Medicine in 2015.

Working Together: A Brief History

Successful collaborations between SBS researchers and the IC have run the gamut from fundamental research into human–computer teaming and human cognition to applied work that facilitates cross-cultural and wartime operations. During World War II, the Office of Strategic Services—the nation's first foreign intelligence agency and the precursor to the Central Intelligence Agency (CIA)—hired political scientists, psychologists, anthropologists, sociologists, and economists to support such functions as analyzing foreign intelligence, assessing enemy and allied morale, screening and training intelligence operatives, calculating the enemy's military capacity, and identifying optimal bombing routes and payloads (O'Rand, 1992). Similarly, anthropologists and psychologists working at the Office of War Information (OWI) provided insights into the cultures and values of foreign populations relevant to the war effort. Anthropologist Ruth Benedict's groundbreaking and best-selling study of Japanese culture, *The Chrysanthemum and the Sword*, which began as an OWI report, influenced the values and design of the United Nations when it was established at war's end (Mandler, 2013).

Wartime projects benefited SBS scholarship even as they served national security. For example, political scientist Harold Lasswell's studies of international political opinion and morale for the Wartime Communications Research Project were widely recognized as proving the value of large-scale, quantitative methods for studying communication (Backhouse and Fontaine, 2010; Rohde, 2013). Likewise, during and after World War II, the Office of Naval Research helped support the development of field theory in sociology through its financial support for the Massachusetts Institute of Technology (MIT) because it hoped to learn about group dynamics and the ways people identify with each other as members of a particular group (O'Rand, 1992, p. 190).

Federal investments in SBS research expanded in scale and scope in the second half of the 20th century. These investments demonstrate that the intelligence and security communities have consistently supported a spectrum of SBS research, from fundamental scientific investigations to scholarship with direct applications to intelligence and related security activities. In the applied domains, for example, research at the RAND Corporation facilitated new understandings of human decision making derived from game theory, social psychology, and systems analysis. These insights fostered and supported nuclear deterrence strategies that helped keep the Cold War cold in the United States and Europe.

Such efforts have parallels today. For example, SBS researchers work in partnership with intelligence and military agencies to enhance cultural and linguistic knowledge. Drawing on basic research in communications, cul-

tural anthropology, political science, social psychology, and sociology, for instance, the Marine Corps Center for Advanced Operational Culture and Language provides the security community with concepts and skills that facilitate cross-cultural understanding (National Academies of Sciences, Engineering, and Medicine, 2017, p. 23).

Recognizing a need for more sustained investment in SBS research relevant to counterterrorism and counterinsurgency in the 21st century, the secretary of defense created the Minerva Research Initiative in 2008. This initiative bridges basic and applied SBS research by supporting unclassified social science research that improves "basic understanding of the social, cultural, behavioral, and political forces that shape" strategically important regions of the globe.[3] Funded projects include studies of social, cultural, economic, and psychological factors that affect radicalization; the role of cybermedia in state stability; and the impacts of environmental, economic, social, and political factors on conflict and instability among both state and nonstate actors.

The Defense Advanced Research Projects Agency (DARPA) began funding research on machine-aided cognition and human–computer communication in the early 1960s. The first director of DARPA's behavioral sciences and computer science division, psychologist and computer scientist J.C.R. Licklider, articulated a vision of human–computer symbiosis in 1960 that is still relevant today. He wrote, "in not too many years, human brains and computing machines will be coupled together very tightly . . . the resulting partnership will think as no human brain has ever thought" (Licklider, 1960, p. 4; Norberg et al., 1996). DARPA has funded research that has produced major advances. For example, its funds contributed to the creation of PLATO (Programmed Logic for Automatic Teaching Operations), which, first released in 1972, harnessed research in psychology to revolutionize computer-based education (Dear, 2017). More recently, IC investments in social network analysis have generated methodological breakthroughs.

Together with the Intelligence Advanced Research Projects Activity (IARPA)—created by ODNI in 2006—DARPA continues to support research that combines computational tools with SBS knowledge to develop social forecasting techniques and other approaches to improved human and organizational decision making. This research has been foundational to the development of such systems as the Worldwide Integrated Crisis Early Warning system, which uses natural language processing, modeling, and other methods to track international events and forecast political instability (NASEM, 2017, p. 22).

The research portfolios of DARPA and IARPA also include support for research in the decision sciences, cognitive science, and other SBS areas

[3]Available: https://basicresearch.defense.gov/minerva [February 2019].

with the potential to enhance basic and applied knowledge that can contribute to both national security and scientific knowledge (Defense Advanced Research Projects Agency, 2018; Office of the Director of National Intelligence, 2018). In addition to providing new computational tools for monitoring and forecasting of global events, these research portfolios advance SBS knowledge about human judgment and decision making in high-stakes and rapidly changing environments.

One recent example of such contributions, discussed in Chapter 7, is the Good Judgment Project (Office of the Director of National Intelligence, 2015). Developed by scholars at the University of Pennsylvania and the University of California, Berkeley as part of IARPA's forecasting tournaments (which ran annually from 2011 to 2015), the project generated results valued by both IARPA and SBS researchers and has been adopted by the National Intelligence Council. The project demonstrated the validity of forecasting tournaments as predictive tools and provided IARPA with insights into best practices for designing and running such tournaments. It also produced results directly relevant to the SBS research community broadly, including the identification of mechanisms for quantifying good judgment and methods for facilitating it, such as cognitive debiasing, providing incentives for accuracy, and designing predictive questions that facilitate accuracy. Notably, both researchers and project managers have been careful not to oversell the results of their findings (Rohde, 2017, pp. 792–813). Previous predictive projects had claimed more accuracy and foresight than they were able to provide. By contrast, researchers involved in the Good Judgment Project have stressed that their work shows that prediction is currently most accurate for approximately 1 year into the future, rather than longer timespans (Chen, 2015; Tetlock et al., 2014, pp. 290–295).

The above research investments run parallel to research in other high-stakes professional domains, such as medicine and finance, in yielding promising insights that can improve judgment and performance. SBS research has shown that human cognitive fallibilities, such as hindsight bias (the unsubstantiated belief that one could have predicted an event) and outcome bias (the tendency to judge decisions by how they turned out rather than by how thoughtfully they were made) hinder learning in workforces. These findings have led to the development of new methods for facilitating the reduction of biases in thinking in high-stakes situations by better identifying sources of failure in judgment and decision making (National Research Council, 2012, pp. 15–16).

Lessons for Productive Collaboration

The examples of productive collaboration discussed in this report demonstrate that the partnership between the IC and the SBS community

has often been successful when research, whether basic or applied, has advanced knowledge of mutual interest to both communities. The relationship between SBS researchers and the national security community has not always operated as smoothly as in these examples, however. We examine here a few cases in which problems arose so as to draw lessons for future collaborations.

Careful attention to transparency in funding relationships on both sides has helped restore the public reputation of joint efforts, as well as protect the integrity of the products of joint research.

During the early years of the Cold War, the need for research-based information was great, but security concerns were also heightened. On some occasions, normal protocols for transparency and accountability were not observed, and financial and other ties between SBS researchers and the IC were hidden from the public (Rohde, 2013). This lack of transparency caused problems within both communities, as illustrated by the experience of MIT's prestigious Center for International Studies. The center, which had the mission of applying "social science to problems bearing on the peace and development of the world community" (Gilman, 2004, p. 159), was established in 1951 in large part with secret CIA funds. For the next 15 years, the center's researchers produced some of the most influential work in modernization theory, international communications, and development studies without disclosing their relationship to the IC. Despite being questioned, they denied any ties to the CIA until investigative journalists produced unequivocal proof in 1966, at which time MIT terminated its relationship with the agency (Rohde, 2013). The American Political Science Association's integrity was similarly compromised when social scientists learned that the association's longtime executive director disguised ideological statements as scholarship and founded a private research corporation that secretly took CIA money (Oren, 2002).

While less common, programs that used or appeared to use SBS as a cover for IC programs also contributed to public suspicion of SBS–IC collaboration. From 1955 to 1962, for example, a Michigan State University program that allegedly provided public administration training in South Vietnam served as cover for a CIA-funded counterespionage training program that was implicated in accusations of torture and assassination in South Vietnam.

SBS researchers and the IC have taken these experiences to heart. It has been decades since collaborations between the two communities have been marred by evidence of covert funding.

Explicit attention to balancing scientific norms and procedures with the need to protect security in the design and execution of research benefits both the researchers and security agencies involved.

The agencies that fund and use SBS research face the challenge of balancing their own needs with the desire of academic researchers to advance intellectual developments in their fields. As noted in a recent report by the Institute for Defense Analyses, when the goals of a research program are ambiguous, or when the uses to which funding agencies will put the research are unclear, particularly in relation to the program's security or intelligence mission, the program is more likely "to sow seeds of mistrust" between the two communities (Koonin et al., 2013, p. 12). While the Good Judgment Project, discussed above, provides an example of successful balancing of agency and SBS needs and interests, examples of failure provide instructive lessons for future collaboration.

One such example is Project Camelot, an ambitious, unclassified, multidisciplinary study of political revolution in Latin America during the Cold War. The project, funded by the U.S. Army and DARPA, was designed to identify the causes of communist insurgency to facilitate prediction of the onset of revolution. The project attracted international criticism in 1965 when press accounts in several Latin American countries where the work was being carried out revealed that researchers affiliated with the work had misrepresented it to potential research partners in those countries as a foundation-supported effort. Journalists in several of the countries involved argued that these events proved that the U.S. government used SBS research as a cover for intelligence gathering and espionage (Rohde, 2013).

The National Research Council concluded that Project Camelot demonstrated "that military sponsorship of social science research pertaining to the internal politics of other nations may have adverse repercussions on American foreign policy" (National Research Council, 1971, p. 7). The accusations directed at the project triggered congressional hearings into the military's research programs, prompting the Army to cancel the project abruptly so as to avoid further scrutiny and embarrassment (Rohde, 2013; Zehfuss, 2012).

Project Camelot also was emblematic of the failure of SBS researchers and their sponsors to balance scientific and national security goals. Critics in the SBS community argued that the project's core problem was that its researchers converted SBS research to militarized language and goals, thereby subverting the natural direction of research and introducing politics into science. Critics argued that researchers and their sponsors had brought "the whole of social sciences under the heading of counter-insurgency" by framing the research questions in military terms—as studies of counter-insurgency, guerrilla warfare, and the like (Rohde, 2013, p. 84). As the National Academy of Sciences concluded at the time, government agencies

and researchers could improve their relationship by assuming more responsibility for stating needs in terms that are meaningful to the investigator rather than the military (National Research Council, 1971).

The funders of Project Camelot had reasons to be critical of their SBS partners as well. For example, they had to intervene during the study's planning phase when social scientists proposed including studies of the French Canadian separatist movement in their investigation (Rohde, 2013, pp. 70–71). Experts on counterinsurgency research at DARPA and members of the Defense Science Board pointed out that the project would likely have failed on its own merits. Months before it attracted public attention, government officials worried that the researchers directing the project had not produced a clear research plan, but instead listed only "generalities . . . about research hypotheses" and "vague and formless" descriptions of the project's methodology (Deitchman, 1976, p. 146).

SBS research projects during the Vietnam War era also include cases in which government funders were let down by SBS researchers who failed to provide rigorous and relevant expertise. In 1967, for example, DARPA hired the research group Simulmatics Corporation—which was led by an MIT political scientist and staffed by reputable SBS scholars—to study social relationships in South Vietnamese hamlets and determine what motivated support for the North and South Vietnamese causes. Government experts found that the studies seemed as if "someone had taken a book of rules about scientific methodology, then systematically violated each one" (Weinberger, 2017, p. 179). A study of communications and propaganda, for example, yielded results that DARPA officials found were riddled with contaminated variables and violations of basic rules of inference.

Camelot and Simulmatics were military-sponsored, not IC, projects. Nevertheless, their histories point to the fact that the partnership between the SBS community and the IC may be weakened when research priorities, methods, and administration fail to meet the needs, standards, and values of both collaborators. Achieving that balance is difficult even when research is carried out with sufficient scholarly integrity and careful management.

Recent examples indicate that members of both communities have become more successful in balancing their mutual needs, standards, and values. For example, SBS researchers criticized the U.S. Department of Defense (DoD)–funded Minerva Research Initiative in its first year for defining research areas that leaned too heavily toward national security concerns, which thus failed to appeal to many relevant researchers (Gearty, 2008). They also criticized the program for its grant review process, which initially was performed internally within DoD rather than through peer review. In subsequent years, Minerva program managers responded to these concerns and incorporated substantial scholarly input into the processes for setting research priorities and reviewing grants (Krebs, 2008).

Relationships between research universities and the IC can be complicated in other ways as well. A 2017 book documents cases in which members of the IC have enrolled in university programs in an undercover capacity—so that at least their fellow students were not aware of their official role—and of cases where students who were foreign nationals took advantage of access to research for the benefit of their governments (Golden, 2017).

It is important to recognize that not all SBS researchers view partnerships between their community and the IC in the same way. Researchers may have differing expectations for fundamental and applied research conducted in this context, or for classified as opposed to unclassified research. Furthermore, researchers' interpretation of the appropriate balance between scholarship and application can differ across and within scholarly disciplines. While many scholars see DARPA and Minerva programs as well balanced, some criticize such efforts for implicitly favoring narrow and short-term American interests and unwittingly supporting "non-democratic actions or governments" (Koonin et al., 2013, p. 11). Scholars in the fields of anthropology, political science, and international relations have been particularly critical of security-funded research, while scholars in other fields have embraced collaboration more fully (Zehfuss, 2012).

The SBS–IC relationship can become strained when clarity or consensus with respect to values and the ethics of research projects and programs is lacking. Respecting ethical norms for research will require that members of the SBS community and the IC engage in ongoing dialogue concerning research ethics in new research domains.

Research endeavors in which both academics and members of the IC take part or have a stake can highlight differences between the two cultures (see Chapter 2) and raise sometimes challenging questions. The development of complex and sophisticated technologies adds another layer of complexity to many questions about research protocols and ethics. We look briefly here at three key issues: ethics and values in a research context, emerging ethical standards in a world of big data, and the reproducibility of research findings.

Ethics and Values in a Research Context

Neither SBS research nor intelligence analysis is a value-free enterprise. Like all researchers, those in SBS fields must be aware of and articulate the influence of values in their work. The values of scientific objectivity and rigor are paramount for most researchers, but values come into play as well in the selection and definition of research questions to pursue. Scholars investigating the effects of poverty on children, for example, recognize

that they regard promoting children's welfare as an undisputed good, just as medical researchers regard protecting or restoring health as a noncontroversial objective.

More complex and subtle values and assumptions may arise in research that is relevant to national security issues. For example, researchers working on national security issues agree that protecting democracy is a positive good, but they may disagree about whether certain research programs or policies embody those values. Social scientists who assisted stability operations of the U.S. military in Iraq and Afghanistan, for instance, argued that their research made Americans, Iraqis, and Afghanis safer, but other social scientists argued that the research only facilitated military operations and did not serve science or democracy (Zehfuss, 2012). While researchers will likely continue to disagree about national security policy, clear and open communication about objectives and the relationship between research and application may help build and maintain trust between SBS researchers and the IC even in the face of policy disagreement.

If history is a good indicator, scrutiny of SBS research and its relationship to government is more likely to arise in contexts of heightened political and other sensitivities. During some periods—the 1940s and 1950s, for example—Americans have largely shared a public consensus as to American strategic and security interests. At such times, collaborations between the SBS community and the IC have attracted very little attention or concern. During the 1960s, however, especially as dissent related to U.S. policies in Vietnam grew, the IC–SBS collaboration faced greater public scrutiny. During congressional hearings in 1968, for example, Senator William J. Fulbright linked U.S. failures in the Vietnam War to the security community's SBS research investments. As a result, congressional appropriations for security community–funded SBS research dropped from $40 million in 1967 to $13.7 million in 1969 (Rohde, 2013).

Similar challenges are apparent today. Revelations about controversial intelligence practices in the first decade of the 21st century—from extraordinary rendition;[4] to the National Security Agency's bulk data collection programs; to harsh interrogation methods, including methods based in psychological research (Voosen, 2015)—also have fostered concerns about intelligence and security practices among the public. While these practices do not pertain directly to research relevant to the capabilities of intelligence analysts, they may seed mistrust in or heightened scrutiny of the SBS–security community relationship (Goolsby, 2005; National Research

[4]Extraordinary rendition is a policy first used by the United States in the early 1990s in which foreign nationals who are suspected of involvement in terrorist-related activities are detained on foreign soil for interrogation in U.S. facilities or those of another country; see https://www.aclu.org/other/fact-sheet-extraordinary-rendition [January 2019].

Council and National Academy of Engineering, 2014; Zehfuss, 2012) This report appears at a time when questions related to terrorism, immigration, cybersecurity, and many other issues keep those concerns very current. Practices that build trust, including transparency in funding and clarity about research methods, goals, and applications, may help mitigate such concerns and strengthen ties. Examination of the relationship between academics and the IC has prompted several social science disciplines to embrace the recommendation that unless a national emergency presents an overriding need, the following activities should be avoided (Johnson, 2019, p. 17):

- agency covert recruitment on campus;
- covert research relationships;
- the use of academic cover by intelligence officers;
- the tasking of faculty and students to collect intelligence; and
- the tapping of academicians for counterintelligence or covert action operations.

It is also important to recognize that SBS research is valuable to the IC, as well as to other sectors, including education, finance, and medicine, to name but a few, because of its capacity to expand analytic understanding of human emotions, motivations, and actions. But because that understanding can facilitate the shaping and perhaps even the manipulation of emotional responses and perceptions, government-funded SBS research may generate public concern.

One example of such concern arises from the dramatic development of new data sources, such as social media mining and new computational social science techniques that can be used to analyze and possibly shape population sentiments. In 2018, controversy was sparked by revelations that the private research firm Cambridge Analytica was improperly obtaining data on Facebook users and deploying nontransparent and proprietary behavioral technologies to design information campaigns intended to influence human attitudes and actions. Whether Cambridge Analytica's psychographic techniques are scientifically sound or effective is an open question (Gibney, 2018). But scholars, journalists, and public officials have expressed grave concern that the firm's services were or could be purchased by governmental and nongovernmental clients (Cadwalladr and Harrison-Graham, 2018; Lewis et al., 2018; Shaw, 2018; Wildermuth, 2018). This episode demonstrates sensitivities that can accompany the deployment of behavioral technologies. These concerns are likely to remain salient with the growth of computational social science and big data research, including some of the research areas endorsed in this report, because of their valuable applications for protecting security.

Changing norms with regard to research ethics also require attention from SBS researchers and their partners in the IC. The U.S. military's aboveground nuclear exercises, carried out in Nevada from 1951 to 1957 and code-named Desert Rock, illustrate the way changing norms have complicated the relationship. As part of this effort, psychologists seeking to understand soldiers' ability to function in the tactical atomic environment and gauge the risk of panic on the atomic battlefield studied 600 soldiers to assess the psychological impact of witnessing an atomic explosion. While the soldiers were informed of the risks of radiation exposure and reassured that the exercises were systematic, the research design and scientific utility of the tests were the subject of internal disagreement among military officials. Military officials also disagreed about an emerging ethical question: whether the test subjects should be considered volunteers to whom risks were disclosed or soldiers involved in training (Advisory Committee on Human Radiation Experiments, 1995).

At the time of this research, the 1950s, attitudes in the country with respect to large institutions, including both the military and scientific establishments, were in a state of transition. There was little public comment on this research at the time. Public controversy about the physical effects of the blasts on the "atomic soldiers" emerged only decades later as norms for human subjects protections changed.

A more contemporary example is DARPA's Brain Machine Interface program, which has generated debate among neuroscientists (Moreno, 2012). Some pointed to the program's potential medical benefits, including treatments for degenerative neurological diseases. Other researchers argued that DARPA-funded researchers were conducting research that would support the development of human enhancements, such as "brain–machine interfaces," that would be used to enhance performance on the battlefield, which many regard as unethical (Hoag, 2003; National Research Council, 2008, 2009; Rudolph, 2003; Silence of the Neuroengineers, 2003). Another example is so-called enhanced interrogation: in the wake of the September 11, 2001, attacks, psychologists helped the CIA establish and carry out a program of interrogation of suspected terrorists that included methods regarded by many as torture, which led to a highly critical investigation by the Senate Select Committee on Intelligence (U.S. Senate Select Committee on Intelligence, 2014; see also Pfiffner, 2010), as well as policy statements by the American Psychological Association. One of the methods, waterboarding, was used by Japanese soldiers interrogating captured U.S. soldiers during World War II, for which they later went to prison (Johnson, 2018).

Such examples demonstrate how important it is that research sponsors consider researchers' positions and evolving perspectives so as to avoid proposing and supporting projects that cross ethical lines. Clear statements of

mission intent also help sponsors and researchers avoid misunderstandings about the implications or goals of research programs (Moreno, 2012). SBS researchers are concerned about ensuring that their research does not cause unnecessary harm, but the relationship between research and potential harm is often unclear—and itself is the subject of unresolved debate. These episodes are instructive because this report is emerging at a time when the ethics of research using big data are also under scrutiny and in flux.

Emerging Ethical Standards in a World of Big Data

Advances in computational social science are offering exciting new possibilities for IC-related SBS research, including enhanced analysis of open-source intelligence such as social media data, data collected from sensors, and other digital information produced by routine human actions and behaviors (Harman, 2015). This information is often granular, is durable, and can be shared across institutional and national borders at high speeds. Research conducted using such data has the potential to cause harm to the individuals whose information or attributes are collected, including the loss of privacy and of individuals' autonomous control over their personal information.

While SBS researchers have long been accustomed to addressing research ethics via the Common Rule (a federal policy statement regarding the protection of human subjects involved in research), computational social science research transcends traditional human subjects protections and raises a number of new ethical questions. For example: Are data subjects the same as human subjects, or are they different? What reasonable expectations of privacy do people have with respect to their digital traces, and how do those expectations change in different digital venues? Is informed consent possible, realistic, or required in big data research? Researchers and ethicists stress that these questions do not have straightforward answers (Buchanan, 2017; Zook et al., 2017). Furthermore, because digital collection tools are proliferating, because digital methods are changing rapidly, and because machine learning tools create decision rules that may not be transparent or intuitive, digital research may generate new and unexpected ethical questions.

These issues are discussed in detail in Appendix D, but we note here that they are especially salient when data are collected or analyzed in a national security context. Internet users typically do not know what traces of their everyday lives are monitored; what happens to their information; or what, if anything, happens because of it. The potential for surveillance by the security community afforded by digital data compounds the power

imbalances already present in digital spaces. As discussed above, failure to address ethical concerns can have a chilling effect on research; the public may lose its trust in the SBS research community, as well as in the government agencies that sponsor such research, including the security community. In the digital context, widespread concern that the Internet is a space where actions are monitored, stored, and analyzed rather than a site of free information exchange also may cause people to censor their online behavior, with a chilling effect on Internet use itself (Brunton and Nissenbaum, 2015; Mayer-Schönberger, 2011; Penny, 2016). Researchers and the IC will continue to grapple with the need to balance privacy and autonomy on the one hand and security on the other (Walsh and Miller, 2016). These domains both overlap and conflict, and navigating this terrain will require careful attention to evolving ethical norms and values.

Reproducibility of Research Findings

Questions about the reproducibility of research results, not only in SBS fields but also across the sciences, have implications for intelligence analysis. The reproducibility of results and testing for generality are key ways in which researchers confirm that their findings are valid; these steps are regarded as keystones of the scientific method. Studies completed over the past decade, however, have pointed to the widespread difficulty of replicating results in numerous fields, such as medicine, big data and computation, and biometrics and behavior metrics. In science, as in national security, any index or finding may fail to replicate precisely because of intrinsic limits in measurement; in some cases, more valid conclusions may be derived from measures other than those originally used. The research community is focused on identifying best practices for enhancing both reproducibility and validity (see Appendix C for a more detailed discussion).

A consensus committee of the National Academies has examined this issue,[5] but it is clear that the importance of understanding and quantifying the reliability of information and of determining how best to process and display the information and integrate or aggregate information from multiple sources will influence emerging SBS research in the coming decade. The robustness and validity of new data, modeling, and theory development are also important in answering researchable questions related to national security, and it will therefore be important for the IC to consider these issues carefully in planning its own empirical efforts.

[5]Information about the study can be found at http://sites.nationalacademies.org/dbasse/bbcss/reproducibility_and_replicability_in_science/index.htm [December 2018].

CONCLUSIONS

The committee saw ample evidence of the productive potential of collaboration between the IC and the SBS research community. We offer three conclusions regarding the elements needed for productive collaboration.

CONCLUSION 9-1: Explicit attention to the respective intellectual goals, values, and perspectives of members of the Intelligence Community (IC) and academic researchers is a prerequisite for productive collaboration. Collaborations between the two have yielded important scientific and analytic insights, and have functioned well when funding sources and agency goals have been transparent, when social and behavioral sciences research questions and agency missions and goals have been harmonized and clear, and when ethical and value-based concerns have been treated with sufficient care. Conversely, the relationship has fractured in the past when funding sources have been kept secret or misrepresented, researchers and government agencies have struggled to balance research and agency needs, and research has touched on broader ethical or value-based disagreements.

CONCLUSION 9-2: Ethical issues may arise at all steps of the research process, from planning, to dissemination of findings, to the operationalization of digital tools in analytic contexts. Because standards with respect to some ethical issues—particularly those concerning the use of large-scale digital datasets—are developing, and because these issues are context-sensitive, ethical assessments require careful attention throughout the research process.

CONCLUSION 9-3: Meticulous clarity and openness about the approaches taken to ensure the reproducibility and validity of the evidence generated in the course of research conducted by or with the support of the Intelligence Community (IC) are critical to the utility of the research results. The IC can promote this standard by requiring researchers to identify project components that incorporate assessments of reproducibility, replication, and validity.

REFERENCES

Advisory Committee on Human Radiation Experiments. (1995). *Final Report of the Advisory Committee on Human Radiation Experiments* (No. 061-000-00-848-9). Washington, DC: U.S. Government Printing Office. Available: https://www.osti.gov/opennet/servlets/purl/120931/120931.pdf [December 2018].

Backhouse, R., and Fontaine, P. (2010). *The History of the Social Sciences since 1945*. Cambridge, UK: Cambridge University Press.

Barabási, A.L., and Bonabeau, E. (2003). Scale-free networks. *Scientific American, 288*(5), 60–69.

Bersin, J. (2017). Robotics, AI and cognitive computing are changing organizations even faster than we thought. *Forbes*, March 9. Available: https://www.forbes.com/sites/joshbersin/2017/03/09/robotics-ai-and-cognitive-computing-are-changing-organizations-even-faster-than-we-thought/#2b7db67fa3f4 [December 2018].

Borgatti, S.P., Mehra, A., Brass, D.J., and Labianca, G. (2009). Network analysis in the social sciences. *Science, 323*(5916), 892–895.

Broido, A.D., and Clauset, A. (2018). Scale-Free Networks Are Rare. *arXiv:1801.03400*. Available: https://arxiv.org/abs/1801.03400v1 [December 2018].

Brookey, R.A. (2007). The format wars: Drawing the battle lines for the next DVD. *Convergence: The International Journal of Research into New Media Technologies*, *13*(2), 199–211.

Brunton, F., and Nissenbaum, H. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.

Buchanan, L. (2017). *Brief Overview of the Revised Common Rule and Subpart B—Pregnant Women*. Washington, DC: Office for the Human Research Protections. Available: https://www.nichd.nih.gov/sites/default/files/2017-11/4-OverviewNew_Rule_SubpartB.pdf [December 2018].

Burger, J. (2017). *The Health of People: How the Social Sciences Can Improve Population Health*. London, UK: SAGE Publications.

Cadwalladr, C., and Harrison-Graham, E. (2018). 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, March 17. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [December 2018].

Chen, A. (2015). Seeing into the future: Does Philip Tetlock hold the key to accurate predictions? *The Chronicle Review*, October 5. Available: https://www.chronicle.com/article/Philip-Tetlock-s-Tomorrows/233507 [December 2018].

Dear, B. (2017). *The Friendly Orange Glow: The Untold Story of the Rise of Cyberculture*. New York: Penguin Random House

Defense Advanced Research Projects Agency. (2018). *Our Research*. Available: https://www.darpa.mil/our-research [December 2018].

Deitchman, S. (1976). *The Best-Laid Schemes: A Tale of Social Research and Bureaucracy*. Cambridge, MA: The MIT Press.

Gearty, C. (2008). Skewing scholarship. *The Social Science Research Council*, October 9. Available: http://essays.ssrc.org/minerva/2008/10/09/gearty [November 2018].

Gibney, E. (2018). The scant science behind Cambridge Analytica's controversial marketing techniques. *Nature News Explainer*, March 29. Available: https://www.nature.com/articles/d41586-018-03880-4?utm_source=twt_nnc&utm_medium=social&utm_campaign=naturenews&sf185785067=1 [November 2018].

Gilman, N. (2004). *Mandarins of the Future: Modernization Theory in Cold War America*. Baltimore, MD: Johns Hopkins University Press.

Golden, D. (2017). *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities*. New York: Henry Holt and Company.

Goolsby, R. (2005). Ethics and defense agency funding: Some considerations. *Social Networks, 27*(2), 95–106.

Grindley, P. (1990). Winning standards contests: Using product standards in business strategy. *Business Strategy Review, 1*(1), 71–84.

Harman, J. (2015). Disrupting the Intelligence Community: America's spy agencies need an upgrade. *Foreign Affairs,* March/April. Available: https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community [November 2018].

Hauch, V., Blandón-Gitlin, I., Masip, J., and Sporer, S.L. (2015). Are computers effective lie detectors? A meta-analysis of linguistic cues to deception. *Personality and Social Psychology Review, 19*(4), 307–342.

Heathcote, A., Brown, S., and Mewhort, D.J.K. (2000). The power law repealed: The case for an exponential law of practice. *Psychonomic Bulletin and Review, 7*(2), 185–207.

Hoag, H. (2003). Remote control. *Nature, 423*(6942), 796–798. doi:10.1038/423796a.

Johnson, L.K. (2018). *Spy Watching: Intelligence Accountability in the United States*. New York: Oxford University Press.

Johnson, L.K. (2019). Spies and scholars in the United States: Winds of ambivalence in the groves of academe. *Intelligence and National Security*, *34*(1), 1–21. doi:10.1080/02684527.2018.1517429.

Jones, J.H., and Handcock, M.S. (2003). Sexual contacts and epidemic thresholds. *Nature, 423*(6940), 605–606.

Koonin, S., Keller, S.A., Shipp, S.S., Allen, T.W., and Walejko, G.K. (2013). *Pathways to Cooperation between the Intelligence Community and the Social and Behavioral Science Communities* (Analyses Paper P-5000). Alexandria, VA: Institute of Defense.

Krebs, R.R. (2008). Minerva: Unclipping the owl's wings. *The Social Science Reseach Council*, November 19. Available: http://essays.ssrc.org/minerva/2008/11/19/krebs [November 2018].

Lewis, P., Grierson, J., and Weaver, M. (2018). Cambridge Analytica academic's work upset university colleagues. *The Guardian*, March 24. Available: https://www.theguardian.com/education/2018/mar/24/cambridge-analytica-academics-work-upset-university-colleagues [December 2018].

Licklider, J.C.R. (1960). Man–computer symbiosis. *IRE Transactions on Human Factors in Electronics, HFE-1*(1), 4–11. doi:10.1109/THFE2.1960.4503259.

Mandler, P. (2013). *Return from the Natives: How Margaret Mead Won the Second World War and Lost the Cold War*. New Haven, CT: Yale University Press.

Mayer-Schönberger, V. (2011). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

Minerva Research Initiative. (2018). *Minerva Research Initiative*. Available: https://minerva.defense.gov [November 2018].

Moreno, J. (2012). *Mind Wars: Brain Science and the Military in the 21st Century*. New York: Bellevue Literary Press.

National Academies of Sciences, Engineering, and Medicine. (2017). *The Value of Social, Behavioral, and Economic Sciences to National Priorities: A Report for the National Science Foundation*. Washington, DC: The National Academies Press.

National Research Council. (1971). *Behavioral and Social Science Research in the Department of Defense: A Framework for Management*. Washington, DC: The National Academies Press.

National Research Council. (2008). *Emerging Cognitive Neuroscience and Related Technologies*. Washington, DC: The National Academies Press.

National Research Council. (2009). *Opportunities in Neuroscience for Future Army Applications*. Washington, DC: The National Academies Press.

National Research Council. (2012). *Using Science as Evidence in Public Policy*. Washington, DC: The National Academies Press.

National Research Council and National Academy of Engineering. (2014). *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues*. Washington, DC: The National Academies Press. doi:10.17226/18512.

Norberg, A.L., O'Neill, J.E., and Freedman, K. (1996). *Transforming Computer Technology: Information Processing for the Pentagon, 1962–1986*. Baltimore, MD: Johns Hopkins University Press.

O'Rand, A.M. (1992). Mathematizing social science in the 1950s: The early development and diffusion of game gheory. *History of Political Economy, 24*, 177–204.

Office of the Director of National Intelligence. (2015). *The Good Judgment Project*. Available: https://www.iarpa.gov/index.php/newsroom/iarpa-in-the-news/2015/439-the-good-judgment-project [November 2018].

Office of the Director of National Intelligence. (2018). *Getting Started with IARPA*. Available: https://www.iarpa.gov/index.php [November 2018].

Oren, I. (2002). *Our Enemies and Us: America's Rivalries and the Making of Political Science*. Ithaca, NY: Cornell University Press.

Penny, J.W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117. doi:10.15779/Z38SS13.

Pfiffner, J.P. (2010). *Torture as Public Policy: Restoring U.S. Credibility on the World Stage*. Boulder, CO: Paradigm.

Porter, T.M. (1986). *The Rise of Statistical Thinking, 1820–1900*. Princeton, NJ: Princeton University Press.

Rohde, J. (2013). *Armed with Expertise: The Militarization of American Social Research During the Cold War*. Ithaca, NY: Cornell University Press.

Rohde, J. (2017). Pax Technologica: Computers, international affairs, and human reason in the Cold War. *ISIS, 108*(4), 792–813.

Rudolph, A. (2003). Military: Brain machine could benefit millions. *Nature, 424*(6947), 369. doi:10.1038/424369b.

Shaw, T. (2018). The new military-industrial complex of big data psy-ops. *The New York Review of Books*, March 21. Available: https://www.nybooks.com/daily/2018/03/21/the-digital-military-industrial-complex [December 2018].

Siegel, E. (2018). Blatantly discriminatory machines: When algorithms explicitly penalize. *Predictive Analytics World*, September 25. Available: https://www.predictiveanalyticsworld.com/patimes/blatantly-discriminatory-machines-when-algorithms-explicitly-penalize/9697 [December 2018].

Silence of the Neuroengineers. (2003). *Nature, 423*, 787. doi:10.1038/423787b.

Smith, A., and Stirling, A. (2007). Moving outside or inside? Objectification and reflexivity in the governance of socio-technical systems. *Journal of Environmental Policy and Planning, 9*(3-4), 351–373.

Tetlock, P.E., Mellers, B.A., Rohrbaugh, N., and Chen, E. (2014). Forecasting tournaments: Tools for increasing transparency and improving the quality of debate. *Current Directions in Psychological Science, 23*(4), 290–295.

U.S. Senate, Select Committee on Intelligence. (2014). *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, 113th Cong., 2d Sess., December 3, 2014.

Voosen, P. (2015). Damning revelations prompt social science to rethink its ties to the military. *Chronicle of Higher Education*, July 15. Available: https://www.chronicle.com/article/Damning-Revelations-Prompt/231591 [July 2018].

Walsh, P.F., and Miller, S. (2016). Rethinking 'five eyes' security intelligence collection policies and practice post Snowden. *Intelligence and National Security, 31*(3), 345–368.

Weinberger, S. (2017). *The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency That Changed the World*. New York: Knopf Doubleday.

Wildermuth, J. (2018). California elected officials dismayed at use of Facebook data. *San Francisco Chronicle*, March 20. Available: https://www.sfchronicle.com/politics/article/California-elected-officials-dismayed-at-use-of-12769078.php [December 2018].

Zehfuss, M. (2012). Culturally sensitive war? The human terrain system and the seduction of ethics. *Security Dialogue, 43*(2), 175–190.

Zook, M., Barocas, S., Boyd, D., Crawford, K., Keller, E., Gangadharan, S.P., Goodman, A., Hollander, R., Koenig, B.A., Metcalf, J., Narayanan, A., Nelson, A., and Pasquale, F. (2017). Ten simple rules for responsible big data research. *PLoS Computational Biology, 13*(3), e1005399. doi:10.1371/journal.pcbi.1005399.

for a workforce exposed to significant stresses in both offline and cyber-mediated environments.

CAPITALIZING ON THESE OPPORTUNITIES

The ideas discussed in this report highlight the reality that technological and other developments in intelligence analysis that proceed without the benefit of SBS research are likely to be limited in their effectiveness or worse, to result in misleading or distorted analysis. We close the report with our broad conclusion about the research opportunities that show promise for the coming decade and a recommendation for strengthening ties between the IC and the research community.

Research Opportunities

We have described both specific ideas and broad areas of opportunity for the IC to consider as it sets priorities for research in the coming decade that can support growth and development in how the analyst workforce performs its functions and in how that workforce itself is nurtured. There are many important areas—such as linguistics, cultural anthropology, behavioral economics, and learning science—that we were unable to address in this decadal survey, which by its nature could highlight only a few among many promising ideas. It is only through sustained attention to the integration of SBS research into its work that the IC can begin to more systematically take advantage of the full range of what SBS research has to offer. The following conclusion expresses our key message to IC leadership as they set specific priorities for research in the coming decade.

CONCLUSION 10-1: Social and behavioral sciences (SBS) research offers a fundamental—indeed essential—contribution to the mission of the Intelligence Community (IC), a mission that requires understanding of what human beings do, how, and why. The research described in this report amply demonstrates the critical importance of

- **interdisciplinary research—both foundational and applied and domestic and international—designed to take advantage of and integrate theory, methodology, and data from across SBS fields to yield new insights into human behavioral and social processes with relevance to national security;**
- **the integration of basic science and developing research on human behavior and social processes, as well as advances in computational methods for large-scale data analysis, with the expertise of the IC on analytic methods and challenges;**

- **the incorporation of a deep understanding of the IC's challenges into the identification of research questions and hypotheses to be tested, as well as the design and execution of research;**
- **the integration of SBS insights into the design and engineering of technologically based analytic tools; and**
- **translational and applied work to establish the direct utility of SBS research findings for the IC.**

Strengthening Ties Between the IC and the Research Community

This chapter's overview of the research examined in this report demonstrates both the power of the opportunities SBS research offers for the IC and the extent of the challenge of fully taking advantage of these opportunities. These ideas come from an extremely diverse set of academic disciplines: there is no "field" of SBS. This long report addresses only a sampling of potentially relevant SBS research; the contributions to intelligence analysis represented by these opportunities—and the landscape of opportunities we could not discuss here—cannot be realized simply by adding features to existing programs. If SBS perspectives are not fully integrated into the IC's thinking, they will bring limited benefit.

This report has described clear evidence of the IC's attention to SBS research, and valuable mechanisms, such as the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Activity (IARPA) are in place that can sponsor, facilitate, and help the IC utilize this research. However, these efforts remain ad hoc in important ways. While many of the mechanisms in place are stable, others come and go; many valuable efforts are "one-offs." The IC as a whole has not yet developed a means of systematically identifying opportunities in SBS research and ensuring that the potential applications of these opportunities to intelligence analysis are pursued.

Scholars have taken note of the gap between the information, ideas, and theories produced by academic researchers and the exigencies of applying that knowledge in the context of government service.[1] This gap is evident across domains, but some work has addressed its significance for the production and use of intelligence analysis. Literature produced under the umbrella of intelligence studies has produced conclusions about the practice of analysis (see Chapter 4) but has had only limited influence because

[1]An influential book that addresses these issues documents problems with the U.S. strategy in Iraq between 1988 and 1991 and suggests ways in which scholars might develop information that is easier to apply, and policy makers might make better use of available research (George, 1993; see also Desch, 2019).

of the distinct difference between the cultures of the IC and academia (see Chapter 2) (Marrin, 2012; see also Hare and Coghill, 2016).

Strengthening the relationship between the SBS community and the IC is a broad-based challenge that has no single solution, and we recognize that we are by no means the first group to focus on this important challenge. Chapter 9 reviews lessons to be drawn from past collaborations between academic researchers and the IC. Capitalizing on the research opportunities discussed in this report will require the IC to abandon procedures and ways of doing business that have been in place for a long time; we close the report with our suggestions regarding ways the IC can proactively build collaboration with SBS researchers into its work.

RECOMMENDATION 10-1: The leadership of the Intelligence Community should make sustained collaboration with researchers in the social and behavioral sciences a key priority as it develops research objectives for the coming decade. A multipronged effort to integrate the knowledge and perspectives of researchers from these fields into the planning and design of efforts to support intelligence analysis is most likely to reap the potential benefits described in this report.

As the key coordinator of the IC, the Office of the Director of National Intelligence (ODNI) can continue to play an important leadership role in fostering the critical ties. The committee had no empirical foundation on which to base specific recommendations about institutional structures within the IC, and future efforts will need to be considered in light of particular efforts currently under way. Whatever structures are chosen, effective interchange is likely to involve four key ingredients:

1. Identifying and building on successful examples
2. Strengthening bridges between the two communities
3. Providing opportunities for analytic staff to build their knowledge of SBS research
4. Drawing on the principles of human–systems integration

Identify and Build on Successful Examples

As early as 1968, the National Academies noted that bringing SBS research to bear on national problems required bridging the divide between the specialized expertise of researchers and the broad problems faced by government (National Research Council Advisory Committee on Government Programs in the Behavioral Sciences, 1968, p. 46). The Intelligence Community Associates program brings academic specialists together and provides a natural bridge to the SBS community. Other valuable efforts to

bridge the gap between the IC and academia have included the Future of Intelligence Analysis Project, a cooperative effort involving the University of Maryland's Center for International and Security Studies and ODNI, which yielded a two-volume report (Lahneman, 2006). Scholars have made broad recommendations for improving understanding and cooperation, such as encouraging scholars to spend time working in agencies and also encouraging analysts to spend time in academia; boosting the contributions of think tanks, which play a useful role in linking research to practice; and redesigning academic programs focused on intelligence (Marrin, 2012).

There is, however, no one office within the IC whose primary function is to survey the SBS landscape for promising research. The Intelligence Community Associates program and other efforts to support collaboration are a valuable resource for the IC and provide the platform on which to build stronger collaboration. One promising approach is the development of communities of practice by "finding junctures where the interests of the communities overlap sufficiently to create significant benefits for both," an objective recommended in a recent Institute for Defense Analyses report (Koonin et al., 2013). A few examples are highlighted in Boxes 10-1, 10-2, 10-3, and 10-4.

BOX 10-1
Community of Practice:
The Defense Science Study Group (DSSG)

Sponsored by the Defense Advanced Research Projects Agency (DARPA), the DSSG identifies new cohorts of talented researchers in the sciences and technology every 2 years. The group meets periodically to confer about research and development challenges facing the national security community. Many DSSG alumni maintain their ties to government, serving as advisors, consultants, and members of special task forces and boards (Koonin et al., 2013; http://dssg.ida.org). While the DSSG has focused primarily on the physical sciences and engineering, a similar program targeted at the SBS community might facilitate translation across the two communities.

BOX 10-2
Community of Practice: The MEDEA Project

A collaboration between the IC and scholars in the environmental sciences offers one model for fostering a community of practice. Through the MEDEA (Measurement of Earth for Environmental Analysis) Project, the IC gave more than 60 environmental scientists access to classified images and data for use in environmental analysis. The project resulted in a number of successes, including the generation of new scientific insights and the public release of more than 860,000 satellite photographs. Perhaps most notably, the project built trust between the research communities and IC. This example suggests that big data research provides a set of problems well suited to facilitating IC–SBS collaboration (Koonin et al., 2013).[a]

[a]For more information about the MEDEA Project, see Johnson (2000).

BOX 10-3
Community of Practice: The Political Instability Task Force

The Central Intelligence Agency (CIA) established the Political Instability Task Force in 1994 in response to the request of senior U.S. policy makers for more social science–based information about the problems of state failure. For more than 15 years, the task force—a collection of mainly university-based social scientists—created quantitative databases, statistical models, and forecasting tools that deepened scholars' and policy officials' understanding of the causes of revolution, ethnic conflict, violent regime change, and genocide (Adler, 2001; McMurtrie, 2014). The work produced by these scholars appeared in dozens of academic research publications and has contributed to social scientific theories about state stability, as well as to methodological advances in international relations (Goldstone, 2001; Goldstone et al., 2010). At the same time, members of the IC have found the task force's forecasts of instability valuable: data collected by the group have, for example, been used to develop the National Intelligence Council's warning list of weak and failing states.[a]

[a]This list has been prepared twice a year since 2005 (Wyler, 2008).

BOX 10-4
Community of Practice:
Laboratory for Analytic Sciences (LAS)

The LAS at North Carolina State University is a successful model of a directly applied research collaboration between the IC and the SBS community. Founded in 2013 by the National Security Agency, the LAS is "a mission-oriented, translational research laboratory" that seeks to "develop new analytic tradecraft, techniques, and technology" for users in the intelligence and defense communities (https://ncsu-las.org/about). This partnership is led by a team that combines deep expertise in both SBS fields and intelligence analysis (https://ncsu-las.org/about). LAS's research has contributed to social scientific knowledge about interdisciplinary research collaborations; it has also created a number of prototypes to facilitate intelligence analysis, including programs that automatically generate textual and visual explanations of incoming data (https://ncsu-las.org/about/accomplishments). Its research programs address important scholarly questions about human cognition, biases, and visualization, as well as research challenges in computational social science, while simultaneously providing translational tools for the intelligence and defense communities.

Strengthen Bridges Between the Two Communities

As discussed in Chapter 2, profound differences between the cultures of the IC and the SBS community reflect their differing missions. One prominent difference is in openness: academic researchers are accustomed to making their data and methods available to other researchers, having their hypotheses and work tested and reviewed, and so on. By contrast, intelligence analysts must work around the need for varying levels of classification.

Some SBS researchers have been reluctant to work on classified projects, which they perceive as placing restrictions on academic freedom, because of their scholarly commitment to open dissemination of research results, and universities have varying policies regarding the acceptance of contracts involving classified research (Goolsby, 2005). The IC worries about classified projects for other reasons, most notably because any expansion of access to classified materials creates the "potential for unintentional disclosure of sensitive intelligence or information about sources and methods" (National Research Council, 2011, p. 23, note 42). Some members of the IC have argued that making the most of open-source intelligence (OSINT) sources and SBS knowledge requires a culture shift, including addressing the problem of classification (Fingar, 2007). One specific illustration of the problem is the requirement that many agencies have for prepublication review and approval of publications derived from research funded by

these agencies, which can inhibit collaboration with SBS academics and may even cause grant proposals to be rejected by university institutional review boards.

Several approaches may be of use in addressing this challenge. For some research purposes, it may be as effective to use a parallel but unclassified source of data. For example, data that once were classified but were later declassified could be made available to the entire SBS research community for comparison of methods and results. It may also be that a review of classification policies by the IC, in consultation with scholars, regarding research needs and objectives could identify policies that could be modified in particular cases.

Apart from issues of classification, means of facilitating productive interactions can play a key role. Possibilities include regular meetings at which members of the two communities share thinking about connections between research issues of concern to the IC, increased funding for unclassified research relating to such issues, and means of continuously soliciting input from researchers and providing incentives for them to pursue topics of interest to the IC. Testbeds, such as the one described in Chapter 7, offer another possibility for forging connections. One advantage to this model, in which researchers and members of the IC collaborate to design, test, and evaluate new projects, is that it can allow researchers access to analysts and their data and tools. Such collaborations can be a venue for research that targets important aspects of the work of the analyst without requiring outside access to classified material.

Provide Opportunities for Analytic Staff to Build SBS Knowledge

Members of the analytic workforce bring a wide range of educational and other experiences when they join the IC. While many have studied or earned degrees in SBS fields, others have not. The nature of their job allows them little time for keeping up with developments in even a single academic field, and little of the classified training they receive is likely to focus on basic SBS research. The committee heard anecdotally of valuable opportunities for analysts to deepen their knowledge of SBS work, including opportunities to take college courses periodically, attend training seminars at conferences, take short courses offered by universities, and participate in training offered by the agencies.

Nevertheless, there is a need for mechanisms through which analysts can keep current on SBS research relevant to their work in focused ways. The volume of relevant SBS research increases continuously, and keeping up even with a single subspecialty relevant to IC concerns could be a full-time job. While individual analysts and institutional units pursue the objective of staying current, we are not aware of any process for ensuring that analysts

working in a particular area can remain abreast of research developments. Possibilities for the IC to consider include working groups developed for the purpose of addressing a particular problem set or theme with SBS dimensions that could allow analysts the opportunity to develop expertise in that area over time. By focusing on such a problem set or theme, the working group could both identify relevant work and pursue individual interests while collaborating with others to build the expertise of the group, establishing themselves as a resource for others. The use of challenge problems, datasets, and artificial social media environments could, for example, support the development and testing of new theories and technologies for cybersecurity.

Other options include the use of such arrangements as the Intergovernmental Personnel Act (IPA) Mobility Program[2] and internship opportunities for Ph.D. candidates that would allow SBS researchers to spend time in the IC and analysts to spend time in academic settings. Such options would require that onerous clearance and classification review constraints be relaxed.

The development of expertise in relevant SBS research could be treated as a core responsibility, and rewarded accordingly. All of these efforts would have the additional benefit of helping researchers build their understanding of the IC.

Draw on the Principles of Human–Systems Integration

Finally, the SBS research identified in this report as relevant to national security is in different stages of operational readiness. Some is still in the basic science stage; some (e.g., many of the ideas for the analyst workforce) is close to translation; and early versions of other research (e.g., social network methods) are in use by the IC. In some cases, new research conducted in the IC context will be needed to assess interventions found to improve teamwork in other settings. Evidence from other contexts for the effectiveness of various interventions can be used as a starting point for the development of interventions for the security community that will need to be tested in the security context.

Once basic research has been evaluated for its applicability in the IC context, it can be translated into operational procedures, methods, or pol-

[2] The IPA program allows for the temporary assignment of personnel between the federal government and outside organizations (e.g., state/local governments, universities, federally funded research and development centers). The Office of Personnel Management notes that although federal agencies do not take full advantage of the IPA program, it is particularly useful in filling positions that require special expertise (e.g., research scientists). The personnel are on detail to the federal agencies and remain employees of their home institutions. See https://www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/#url=Assignment for more information on the IPA program.

icies. This translation requires collaboration among scientists, engineers, analysts, and applied scientists who are adept at the process. The nature of some SBS research (e.g., that in social networks and social cybersecurity) is such that the basic research involves the codevelopment of operational procedures, methods, and theories. In such cases, translational research takes a very different form from that in other areas, such as team science and psychology. Moreover, much of the research that will need to be translated for the IC context in the coming decade will involve interactions among humans and machines, often through social media.

Human–systems integration, an approach developed in the early 20th century, draws on research from numerous SBS domains, including psychology, human factors, management, occupational health and safety, and human–computer interaction, to improve the development of sociotechnical systems (dynamic systems in which people, tasks, technology, and the environment interact throughout the stages of the work the system is to carry out). The goal of this approach is to develop a resilient and adaptive system and avoid unintended consequences (National Research Council, 2007). A human–systems integration approach helps ensure that operational solutions address the needs as well as the capabilities and limitations of the analyst, including limitations that derive from policy decisions.

CLOSING THOUGHTS

Addressing the barriers that interfere with productive collaboration between the IC and the SBS community will require that both communities have realistic expectations; a shared understanding of what SBS research can offer; and an understanding of "the inherent limitations in providing simple, universally applicable answers to complex social science questions," in the words of another National Academies committee, charged with examining the integration of SBS research into the weather enterprise (National Academies of Sciences, Engineering, and Medicine, 2017, p. 6). In 1968, the National Academies argued that bridging the gap between the behavioral sciences and the federal government "requires identifying positions of responsibility in the government where an understanding of the behavioral sciences is essential" (National Research Council Advisory Committee on Government Programs in the Behavioral Sciences, 1968, p. 47).

The IC has unmistakably recognized the importance of SBS research, as its request for the present study demonstrates. Such efforts as the inventory of in-house SBS expertise conducted by ODNI in the wake of the 9/11 Commission Report are further evidence of that commitment (Fingar, 2011). Most recently, the director of national intelligence released a formal strategy for taking advantage of AI and other technologies to augment intelligence, which addresses the importance of "basic research focused

on sense-making" and strengthening collaboration between the IC and research institutions (Office of the Director of National Intelligence, 2019, pp. v and 12). Academic institutions could contribute to the IC–SBS collaboration by devoting greater attention to translational research, supporting the operationalization of tools from the SBS community, and applying SBS research findings to national security needs. The continued strengthening of the IC workforce and the technological systems it needs will depend on interdisciplinary approaches in which the insights and ideas of SBS researchers are fully integrated with the needs and objectives of the IC.

REFERENCES

Adler, R. (2001). The crystal ball of chaos. *Nature, 414*(6863), 480–481.

Desch, M.C. (2019). *Cult of the Irrelevant: The Waning Influence of Social Science on National Security*. Princeton, NJ: Princeton University Press.

Fingar, T. (2007). *Remarks and Q&A by the Deputy Director of National Intelligence for Analysis & Chairman, National Intelligence Council*. Available: https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070717_speech_3.pdf [December 2018].

Fingar, T. (2011). Analysis in the U.S. Intelligence Community: Missions, masters, and methods. In B. Fischhoff and C. Chauvin (Eds.), *Intelligence Analysis: Behavioral and Social Scientific Foundations* (pp. 21–22). Washington, DC: The National Academies Press.

George, A.L. (1993). *Bridging the Gap: Theory and Practice in Foreign Policy*. Washington, DC: United States Institute of Peace Press.

Goldstone, J.A. (2001). Toward a fourth generation of revolutionary theory. *Annual Review of Political Science, 4*, 139–187. doi:10.1146/annurev.polisci.4.1.139.

Goldstone, J.A., Bates, R.H., Epstein, D.L., Gurr, T.R., Lustik, M.B., Marshall, M.G., Ulfelder, J., and Woodward, M. (2010). A global model for forecasting political instability. *American Journal of Political Science*, *54*(1), 190–208.

Goolsby, R. (2005). Ethics and defense agency funding: Some considerations. *Social Networks*, *27*(2), 95–106.

Hare, N., and Coghill, P. (2016). The future of the intelligence analysis task. *Intelligence and National Security*, *31*(6), 858–870. doi:10.1080/02684527.2015.1115238.

Johnson, L.K. (2000). *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*. New York: New York University Press.

Koonin, S.E., Keller, S.A., Shipp, S.S., Allen, T.W., and Walejko, G.K. (2013). *Pathways to Cooperation Between the Intelligence Community and the Social and Behavioral Science Communities*. IDA Paper P-5000. Arlington, VA: Institute for Defense Analyses.

Lahneman, W.J. (2006). *The Future of Intelligence Analysis, Volume I. Final Report*. College Park: The Center for International and Security Studies at Maryland.

Marrin, S. (2012). Is intelligence analysis an art or a science? *International Journal of Intelligence and Counterintelligence*, *25*(3), 529–545. doi: 10.1080/08850607.2012.678690.

McMurtrie, B. (2014). Scoping out the future. *Chronicle of Higher Education*, October 13. Available: https://www.chronicle.com/article/Scoping-Out-the-Future/149271 [December 2018].

National Academies of Sciences, Engineering, and Medicine. (2017). *Integrating Social and Behavioral Sciences within the Weather Enterprise*. Washington, DC: The National Academies Press. doi:10.17226/24865.

National Research Council Advisory Committee on Government Programs in the Behavioral Sciences. (1968). *The Behavioral Sciences and the Federal Government*. Washington, DC: National Academy of Sciences.

National Research Council. (2007). *Human–System Integration in the System Development Process: A New Look*. Washington, DC: The National Academies Press. doi:10.17226/11893.

National Research Council. (2011). *Intelligence Analysis: Behavioral and Social Scientific Foundations*. Washington, DC: The National Academies Press.

Office of the Director of National Intelligence. (2019). *The AIM Initiative—A Strategy for Augmenting Intelligence Using Machines*. Available: https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf [February 2019].

Wyler, L.S. (2008). *Weak and Failing States: Evolving Security Threats and U.S. Policy* (Order Code RL34253). Washington, DC: Congressional Research Service. Available: https://fas.org/sgp/crs/row/RL34253.pdf [December 2018].

Summary

Ten years from now, the job of the intelligence analyst will be transformed. Analysts responding to continuously evolving security risks will likely be tracking new combinations of nonstate and state-sponsored actors who threaten to disrupt governance and civil society. These potential adversaries will likely be motivated by both familiar and unforeseeable drivers, including the effects of global climate change, which will be manifest through such issues as scarcities of water, food, and other resources; extreme weather events; and dislocation of communities. Shifting strategic alliances, military conflicts, the presence of hostile terrorist factions and street gangs, and deteriorating local economies will further challenge stability. At the same time, adversaries and other actors of concern to the Intelligence Community (IC) will have access to new resources, including computing technologies and cyberspace operations, as well as chemical and biological weapons—perhaps even stolen nuclear weaponry—that will dramatically amplify their power to inflict harm and disrupt daily life and commerce.

Intelligence analysts themselves will have new resources based on advances in data processing and other technologies. Technologies including artificial intelligence (AI), large dataset analytics, dynamic search tools, and interactive technologies are already allowing analysts to process and integrate multiple sources of data and intelligence far more quickly and efficiently than ever before. They are also dramatically expanding opportunities for collaboration involving personnel and technology, and integration of new types of data. New knowledge, tools, and technologies with

applications for understanding, forecasting, and mitigating security risks are continually emerging.

The IC will need research from the social and behavioral sciences (SBS) if it is to take maximum advantage of these developing resources and be optimally prepared for the security challenges on the horizon. But what is needed is not simply more research. Intelligence analysts already rely on SBS research, just as they already synthesize large volumes of data and information about fast-breaking developments to produce reliable and accurate assessments that can support urgent and consequential decisions.

To date, however, the influence of SBS research on intelligence analysis has been ad hoc: despite the value of many ongoing efforts, the IC has not found ways to systematically integrate research and perspectives from the academic SBS community into its work. Recognizing this gap and the crucial role of SBS research in supporting intelligence analysis, the Office of the Director of National Intelligence (ODNI), which oversees and directs the work of the agencies and organizations responsible for foreign, military, and domestic intelligence for the United States, requested that the National Academies of Sciences, Engineering, and Medicine conduct a decadal survey of SBS research with applications to national security.

The charge to the Committee on a Decadal Survey of Social and Behavioral Sciences for Applications to National Security was to (1) develop understanding and direction regarding resources from SBS disciplines with the greatest potential to augment and support the intelligence analysis process and enhance national security, which the IC can use in determining its research priorities for the coming decade; and (2) identify lessons to be learned from the application of the decadal survey process in the national security context.

STUDY PROCESS

A decadal survey is a method for engaging members of a scholarly community to identify lines of research with the greatest potential to be of use over a 10-year period in pursuit of a particular goal. The National Academies developed this type of survey to support the planning of future research for other government entities, including the National Aeronautics and Space Administration, the National Science Foundation (NSF), the U.S. Department of Energy, the National Oceanic and Atmospheric Administration, and the U.S. Geological Survey. The process has not previously been used to survey SBS research or to support the IC's research planning. In conducting the present survey, the committee adapted the methods used in previous decadal surveys; we developed a process to seek understanding of the needs of the IC and current challenges in the work of the IC analyst and to cull SBS research of potential relevance to those challenges.

We identified two broad categories of need for the IC: support in leveraging developing research and technology to improve the skills and tools used by analysts, and support in strengthening the IC workforce. Thus, our focus was on the insights provided by the SBS disciplines into human behavior, capacities, and limitations, and ways in which those insights could be integrated into both the content of intelligence analysis (understanding what people and adversaries do) and the technical means of analysis (improving and supplementing the human capacities of the analyst).

We used four criteria to identify the areas of research with the most promise for direct impact on these two categories of need:

1. the potential for impact on urgent national security priorities;
2. the strength of the supporting evidence base;
3. technical readiness, or the state of development on the continuum from basic research, to field testing and evaluation, to applied research; and
4. the potential to use or develop emerging data sources, methods, or other technical advances with potential to yield significant advances.

We also considered the ethical implications of the research itself and its applications throughout the study process.

OPPORTUNITIES TO SHAPE THE FUTURE OF INTELLIGENCE ANALYSIS: RESEARCH DIRECTIONS

Opportunities in the research we examined can contribute to the most fundamental aspects of the IC's work. To adapt to anticipated changes in both the security landscape and the way intelligence analysis is conducted, the IC will need the insights that come from deep understanding of cultural and political history and context, the way humans and social and political entities behave, and current trends and forces shaping the actions and decisions of individuals and groups. Integrating the understanding of human beings and social processes that comes from SBS research into the analyst's work as it evolves in the coming decade will be critical.

It is this knowledge base that will enable the IC to develop tools and methods that are both proactive and interactive and can effectively augment the capacities of human analysts, and, more broadly, to respond effectively to the security threats of the coming decades. We have identified research directions, summarized in our conclusions, for pursuing the opportunities in the bodies of work we examined. While there are clear, critical potential benefits to the IC in each of these areas, they are by no means the only promising ones. Nevertheless, a 10-year research agenda based on these

areas would contribute significantly to the IC's analytic responsibilities, and build a strong foundation for significantly strengthening interchange between the security community and the external SBS research community.

Targeted SBS research offers the potential for stronger intelligence assessments, tools and technologies optimally designed for human use and human–machine interaction, and optimal readiness to confront evolving security threats.

Stronger Intelligence Assessments

SBS research can support the development of intelligence assessments that are **richer** 10 years from now because analysts will have the capacity to use new types of information and analyze existing types of information in new ways. SBS research involves gathering reliable and interpretable data on human behavior that does not fall within the expertise of other disciplines. It provides the essential theoretical and empirical bases for designing and using sophisticated methodologies to make complex data meaningful and enrich the analyst's understanding of the social and political worlds. Assessments may also be more **nuanced** because analysts will have tools that allow them to identify intersections and see connections in large-scale datasets that humans alone could not detect.

Assessments may be **more accurate and efficient**. Methodologies and tools described in this report may allow for faster processing of large volumes of data, integration of multiple kinds of data and other analyses, and tracking of developments—capabilities beyond those of human analysts—but only if conceptual frameworks derived from SBS work provide the basis for their design. The result will be improved forecasting and the possibility of efficiently tracking regions, populations, groups, and sources of information. New kinds of indicators based in research on, for example, manifestations of emotion or how extremist narratives exert influence, could help the analyst gauge changes in a political leader's behavior, the developing strength of a minority group's influence, or the cohesiveness of networks within which toxic narratives are spreading, and direct the analyst's attention more swiftly to those developments requiring attention.

CONCLUSION 5-1:[1] Developing research on narratives, social networks, complex systems, and affect and emotion can enhance understanding of primary targets of intelligence analysis, the potential impact of actions taken by the Intelligence Community, and individual and social processes relevant to security threats. This research offers possibilities for new tools, including but not limited to

[1]Conclusions are numbered according to the chapters in which they are introduced.

- **indicators for use in monitoring and detection of key security-related developments;**
- **algorithms for extracting meaning from large quantities of open-source information; and**
- **models for reasoning about the potential implications of various interventions or activities.**

CONCLUSION 5-2: Interdisciplinary, multimethod approaches to integrating insights from social and behavioral sciences fields with sophisticated technological developments will be essential to support the development of new tools for the analysis and interpretation of data and intelligence. The Intelligence Community would benefit from pursuing a portfolio of such research focused on the development of operational methods and tools.

Tools and Technologies Optimally Designed for Human Use and Human–Machine Interaction

Tools and technologies that become operational in the coming decade and beyond—including advances in data processing and AI that support large dataset analytics, dynamic search tools, statistical modeling, and interactivity—will augment the capacities of the human analyst in vital ways, which will necessarily change the nature of human–machine interaction. Insights from SBS fields are essential to the design and development of tools and technologies that

- take advantage of the strengths of both humans and machines;
- allow humans to collaborate productively with machine partners;
- support more accurate assessment and forecasting of human activity; and
- avoid serious unintended practical and ethical consequences.

SBS research offers insights that will be needed to design tools that use AI and machine learning. It could also support the development of an ecosystem for intelligence analysis composed of human analysts and autonomous AI agents, supported by other technologies, with the capacity to derive meaning efficiently from multiple sources of information.

Existing and emerging SBS research can also provide essential support for the procurement of products from the private sector, such as commercially available software programs and other technologies. While these externally produced resources bring important efficiencies and other benefits, careful attention is needed to ensure that they reflect SBS-based insights so they provide the benefits for which they were sought. Technology used

for analysis is only as strong as the understanding of the human behavior it is being used to model or explain.

CONCLUSION 7-1: To develop a human–machine ecosystem that functions effectively for intelligence analysis, it will be necessary to integrate findings from social and behavioral sciences research into the design and development of artificial intelligence and other technologies involved. A research program for this purpose would extend theory and findings from current research on human–machine interactions to new types of interactions involving multiple agents in a complex teaming environment.

CONCLUSION 7-2: A social and behavioral sciences research agenda to support the development of technologies and systems for effective human–machine teams for intelligence analysis should include, but not be limited to, the following goals:

- **Apply methodologies from the vision sciences, the behavioral sciences, and human factors to advances in data visualization to improve understanding of how people extract meaning from visualizations and the functionality of tools designed to present information from large datasets.**
- **Use techniques from social network analysis to better understand how information can be transmitted effectively, as well as filtered among distributed teams of humans and machines, and how the need to use artificial intelligence (AI) to search and filter information can be balanced with the need to restrict access to certain information.**
- **Develop new modes of forecasting that incorporate human judgment with automated analyses by AI agents.**
- **Apply neuroscience-inspired strategies and tools to research on workload effects in a complex environment of networked human and AI agents.**
- **Examine the implications of ongoing system monitoring of work behaviors in terms of privacy issues, as well as potential interruptions to the intrinsic work habits of human analysts.**
- **Extend insights from the science of human teamwork to determine how to assemble and divide tasks among teams of humans and AI agents and measure performance in such teams.**
- **Identify guidelines for communication protocols for use in coordinating the sharing of information among multiple human and AI agents in ways that accommodate the needs and capabilities of human analysts and minimize disadvantages associated with interruption and multitasking in humans.**

CONCLUSION 7-3: The design, development, and implementation of a system of human–technology teams, which would include autonomous agents, for use in intelligence analysis raise important ethical questions regarding access to certain types of data; authority to modify, store, or transmit data; and accountability and protections when systems fail. The Intelligence Community (IC) could best ensure that such systems function in an ethical manner and prepare to address unforeseeable new ethical issues by

- **from the start, incorporating into the design and development process collaborative research, involving both members of the IC and the social and behavioral sciences community, on the application of ethical principles developed in other human–technology contexts to the IC context;**
- **ensuring that all research supported by the IC adheres to the standards for ethical conduct of research; and**
- **establishing a structure for ongoing review of ethical issues that may arise as the technology develops and new circumstances arise.**

Optimal Readiness to Confront Evolving Security Threats

The contributions of SBS research will be vital to the capacity of the United States to react effectively to future risks. Ongoing SBS work is illuminating, for example, the nature of social networks and complex systems, protections against social cybersecurity threats, evolving ways adversaries influence hearts and minds, and the ways individuals are drawn into radicalization and extremism. Developments in numerous SBS fields are building understanding of both familiar and emerging threats. The emergence of new threats in cyberspace is already a profound challenge for the IC, one that can be expected to grow in scale and urgency in the coming decade. The developing field of social cybersecurity has the potential to offer tools, tactics, procedures, and policies for assessing, predicting, and mitigating the impact of adversarial social cyberattacks.

CONCLUSION 6-1: A comprehensive multidisciplinary research strategy for identifying, monitoring, and countering social cyberattacks, predicated on computational social science, would provide significant support for the Intelligence Community's (IC's) efforts to address the social cybersecurity threat in the coming decade. The emerging field of social cybersecurity research can yield insights that would supplement the IC's training and technology acquisition in the area of social cybersecurity threats and foster an effective social cybersafety culture. These insights could support development of the capacity to, for example, detect bots and malicious online actors and track the impact of social cyberattacks.

CONCLUSION 6-2: The Intelligence Community could strengthen its capacity to safeguard the nation against social cyber-mediated threats by supporting research with the objectives of developing

- **generally applicable scientific methods for assessing bias in online data, drawing conclusions based on missing data, and triangulating to interpolate missing or incorrect data using multiple data sources; and**
- **new computational social science methods that would simultaneously consider change in social networks and narratives within social media–based groups from a geotemporal social-cyber perspective; and operational computational social science theories of influence and manipulation in a cyber-mediated environment that simultaneously take into account the network structure of online communities, the types of actors in those communities, social cognition, emotion, cognitive biases, narratives and counternarratives, and exploitable features of the social media technology.**

Finally, SBS research can aid in strengthening the overall effectiveness of the IC workforce, an important aspect of preparedness for the security challenges of the coming decade. To the extent that foundational and current insights from industrial-organizational psychology and related fields have not already been integrated into the IC's personnel management approaches, translational research to identify the applications of a well-developed body of research and practice in this area is likely to be beneficial. Four salient areas for which robust research is available are the selection of applicants likely to be effective in analytic roles, skill development on the job through both formal training and informal learning, means of retaining and engaging effective analysts, and ways of providing support for a potentially stressed and fatigued workforce.

CONCLUSION 8-1: A range of personal attributes—including skills in critical evaluation, writing and presentation, and teamwork; openness to feedback; and a continuous learning orientation—contribute to successful job performance as an intelligence analyst. To strengthen its capacity to select individuals well suited to work as an intelligence analyst, the Intelligence Community (IC) would benefit from

- **regularly updating its assessment of the facets of the analyst's job performance that are of greatest value to the IC and the attributes most useful for selection of personnel for intelligence analysis roles;**
- **having the capacity to measure a broad range of attributes for use in selecting individuals who possess those attributes; and**

- **evaluating the predictive power and potential ethical implications of such assessment devices as digital games, gleaning information about candidates from social media, and using machine learning approaches to extract information from interviews and resumés and develop scoring algorithms.**

CONCLUSION 8-2: A large body of social and behavioral sciences research identifies individual and organizational factors linked to employee retention, including employees' attitudes and engagement, unit cohesiveness, and leader quality, but these factors have not been examined in the Intelligence Community (IC) context. Translational work examining the role of these potential influencing factors could aid in managing retention in the IC.

CONCLUSION 8-3: A systematic review of the degree to which the organizational culture within the agencies of the Intelligence Community supports both organizationally directed training and autonomous learning could provide valuable information that could be used to promote these means of enhancing the skills of the analytic workforce. This review could focus on practices that promote such a culture, including

- **opportunities for workers to receive feedback,**
- **tolerance for error as employees attempt to use new skills,**
- **support and encouragement from supervisors and peers, and**
- **allocation of time for autonomous learning.**

CONCLUSION 8-4: Emerging research indicates that developing tools and methods could be used to assess and mitigate issues related to the effects of work in the high-stress environment of intelligence analysis, including cognitive fatigue, reduced attention, impaired performance, and decreased efficiency. Possibilities include the application of neuroergonomics (e.g., cueing, visual or auditory warning signals, automation); neuroscience (e.g., noninvasive brain stimulation); and neuropharmacology. The development of effective and safe tools and methods ready for implementation would require (1) research on the utility and applicability of these methods in the Intelligence Community environment, and (2) careful consideration of safety and ethical issues related to their use.

CONCLUSION 8-5: To fully benefit from research findings relevant to the development of an optimal analytic workforce, the Intelligence Community (IC) would need to invest in research and evaluation to

guide their application in the context of intelligence analysis. Translating key insights about selection, training, retention of, and support for the IC analytic workforce will in itself require a team approach in which members of the IC, social and behavioral sciences researchers, applied scientists, and others collaborate to help translate the approaches discussed here for the IC context and assess their effectiveness.

CAPITALIZING ON THESE OPPORTUNITIES

The ideas discussed in this report highlight the reality that technological and other developments in intelligence analysis that proceed without the benefit of SBS research are likely to be limited in their effectiveness, or worse, to result in misleading or distorted analysis.

CONCLUSION 10-1: Social and behavioral sciences (SBS) research offers a fundamental—indeed essential—contribution to the mission of the Intelligence Community (IC), a mission that requires understanding of what human beings do, how, and why. The research described in this report amply demonstrates the critical importance of

- **interdisciplinary research—both foundational and applied and domestic and international—designed to take advantage of and integrate theory, methodology, and data from across SBS fields to yield new insights into human behavioral and social processes with relevance to national security;**
- **the integration of basic science and developing research on human behavior and social processes, as well as advances in computational methods for large-scale data analysis, with the expertise of the IC on analytic methods and challenges;**
- **the incorporation of a deep understanding of the IC's challenges into the identification of research questions and hypotheses to be tested, as well as the design and execution of research;**
- **the integration of SBS insights into the design and engineering of technologically based analytic tools; and**
- **translational and applied work to establish the direct utility of SBS research findings for the IC.**

The range of opportunities explored in this report demonstrates both the power of the benefits SBS research offers for the IC and the extent of the challenge of fully taking advantage of these opportunities. Strengthening the relationship between the SBS community and the IC will be critical if these opportunities are to bear fruit. This report offers insights for sustaining this effort in the long term that come both from the experience of

conducting this decadal survey and from a review of the history of collaboration between these two very different communities.

Overall, what initially appeared to be the greatest challenge in conducting this study—a broad charge that required looking across a very wide research landscape—turned out to be the most valuable aspect of the task. The challenge of casting such a wide net in searching for intersections between the needs of the IC and the available SBS research meant that the committee's efforts were not driven by the perspectives of a single discipline and that we had no preconceptions about where to look for relevant work. Further, despite the obvious difficulty of looking across multiple, diverse disciplines, the study process did reveal certain basic elements that would likely have emerged regardless of the methods used in the process. Without a doubt, for example, any attempt to meet our charge would have highlighted the importance of learning more about human–machine interactions, ways to make use of emerging analytics for big data, and the integration of insights about human behavior and group functioning in the pursuit of cybersecurity.

The survey process also allowed us to see firsthand some of the obstacles to integration and collaboration between the IC and the SBS community, and to observe that coordination between the two is less prevalent than would be optimal. Moreover, awareness of the potential applications of SBS research to IC needs is highly uneven across relevant SBS fields, and there is a long way to go in building awareness of these potential applications of their work among the research community.

Most of the opportunities identified in this report will depend on the integration of research from SBS fields with work from technical fields including engineering, computer science, and neuroscience. Technological developments occur in a social and economic context: SBS research is therefore essential to understanding of the potential applications and benefits, risks, and long-term effects of sophisticated technology and to its sound application, despite significant differences in theory and method between these two cultures. Therefore, we make one recommendation to the IC:

RECOMMENDATION 10-1: The leadership of the Intelligence Community should make sustained collaboration with researchers in the social and behavioral sciences (SBS) community a key priority as it develops research objectives for the coming decade. A multipronged effort to integrate the knowledge and perspectives of researchers from the SBS fields into the planning and design of efforts to support intelligence analysis is most likely to reap the potential benefits described in this report.

Although the objectives and perspectives of the SBS research community and the IC are not always aligned, the two communities have always had much to learn from one another. Researchers and members of the IC have differing objectives, face differing challenges and constraints, and operate in contexts that have very different norms and expectations. Nevertheless, collaborations between the two have for decades yielded important scientific and analytic insights.

CONCLUSION 9-1: Explicit attention to the respective intellectual goals, values, and perspectives of members of the Intelligence Community and academic researchers is a prerequisite for productive collaboration. Collaborations between the two have yielded important scientific and analytic insights, and have functioned well when funding sources and agency goals have been transparent, when social and behavioral sciences research questions and agency missions and goals have been harmonized and clear, and when ethical and value-based concerns have been treated with sufficient care. Conversely, the relationship has fractured in the past when funding sources have been kept secret or misrepresented, researchers and government agencies have struggled to balance research and agency needs, and research has touched on broader ethical or value-based disagreements.

CONCLUSION 9-2: Ethical issues may arise at all steps of the research process, from planning, to dissemination of findings, to the operationalization of digital tools in analytic contexts. Because standards with respect to some ethical issues—particularly those concerning the use of large-scale digital datasets—are developing, and because these issues are context-sensitive, ethical assessments require careful attention throughout the research process.

CONCLUSION 9-3: Meticulous clarity and openness about the approaches taken to ensure the reproducibility and validity of the evidence generated in the course of research conducted by or with the support of the Intelligence Community (IC) are critical to the utility of the research results. The IC can promote this standard by requiring researchers to identify project components that incorporate assessments of reproducibility, replication, and validity.

The findings presented in this report provide the foundation for what the committee hopes will become a stable and continuing process by which SBS research can be culled for its relevance to national security challenges, and promising relevant work can be supported and integrated into IC plan-

ning and operations. Effective interchange in the future is likely to involve four key ingredients:

1. building on effective examples of collaboration, such as communities of practice;
2. strengthening cultural bridges between the two communities and addressing institutional obstacles to collaboration;
3. providing opportunities for analytic staff to build their knowledge of SBS research and for researchers to improve their understanding of the IC; and
4. relying on the principles of human–systems integration to facilitate the development of collaborative systems that function effectively.

This report comes at a critical time in the nation's history: new forms of threats, as well as complex new methods and tools for understanding trends and developments, identifying immediate threats, and forecasting future problems, are making the IC analyst's work both more challenging and more critical. Without understanding of the human component of these developments, the IC analyst would be perilously hampered. Capitalizing on the research opportunities discussed in this report will require the IC to abandon procedures and ways of doing business that have been in place for a long time. The continued strengthening of the IC workforce will depend on interdisciplinary approaches in which the insights and ideas of SBS researchers are fully integrated with the needs and objectives of the IC.