International Journal of Intelligence and CounterIntelligence, 27: 42–57, 2014

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2014.842797

Routledge
Taylor & Francis Group

HAMILTON BEAN

The Paradox of Open Source: An Interview with Douglas J. Naquin

The Associated Press (AP) reported on 8 November 2005 that, as part of post-11 September 2001 (9/11) United States intelligence reform efforts, the Director of National Intelligence (DNI) had established the Open Source Center (OSC).[1] Then-Director of the Central Intelligence Agency (CIA), former Florida congressman Porter Goss, described the OSC as a "major strategic initiative and commitment to the value we place on openly available information."[2] Challenging Goss's statement of commitment, the AP asserted that the OSC had actually been created, in part, in order to "elevate a brand of information [open source] that's long been a stepchild in the U.S. spy community."[3] Directed to "collect and study information that's publicly available around the world, including media reports, Internet postings and even T-shirts in Southeast Asia,"[4] the OSC described itself as "the US Government's premier provider of foreign open source intelligence."[5] Visitors to the OpenSource.gov Website were told that the OSC offered authorized government employees and contractors "information on foreign political, military, economic, and technical issues beyond the usual media from an ever expanding universe of open sources."[6]

Dr. Hamilton Bean is an assistant professor in the Department of Communication at the University of Colorado, Denver. His research intersects the fields of organizational communication and security. From 2001 to 2005, he served in management positions for a Washington, D.C.-based provider of analytical support services to U.S. and international clients in government and industry. Since 2005, he has been affiliated with the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a Center of Excellence funded by the U.S. Department of Homeland Security at the University of Maryland.

A subsequent AP report in 2011 implied that, in the six years since the OSC's establishment, the ''stepchild'' had finally earned more respect. Readers were told that hundreds of OSC analysts, government personnel, and commercial partners were poring over ''Facebook, newspapers, TV news channels, local radio stations, Internet chat rooms—anything overseas that anyone can access and contribute to openly.''[7] The AP noted that OSC analysis ''ends up in President Barack Obama's daily intelligence briefing in one form or another, almost every day.''[8] With numerous intelligence successes to its credit,[9] the U.S. government's investment in the OSC appeared to be paying off. Yet, the question remains: How has the Intelligence Community (IC) coped with the immense amount of publicly available information in the digital era? The intent here is to shed new light on that question.

The topic of open source has long interested readers of this journal.[10] Since the OSC's establishment in 2005, several book-length explorations of open source's potentials and limitations have been produced.[11] Seldom, however, do scholarly articles and books concerning open source include the perspectives of the government's top intelligence officials. In 2005 Douglas Naquin became the OSC's first Director, having already served for three years as the head of the new Center's precursor, the Foreign Broadcast Information Service (FBIS). Naquin retired from the CIA in 2012. Here in an interview with me, he offers a candid perspective on open source's recent institutional history.[12]

Commentators have long noted open source's dualistic tendencies, that is, its ''blessings'' and ''curses.''[13] I draw upon organizational theory and the exchange with Mr. Naquin in seeking to clarify those tendencies by pinpointing five associated dialectical tensions. First, I identify two tensions that characterize institutional change vis-à-vis open source: one is the tension between the financial (''material'') resources invested in open source initiatives and the symbolic meaning of open source for IC members and stakeholders; the other is the tension between organizational structures (formal policies and procedures that configure the relationships among organizational elements) and the transformative actions of individuals (their ''agency''). Next, I note three tensions that characterize open source practice: one is the tension between technology-enabled message processing versus the human context that makes those messages meaningful to recipients; another is the degree to which officials and analysts conduct open source as a unique intelligence activity, rather than mere support to other intelligence disciplines. The third tension is between internally produced versus externally produced (''outsourced'') open source collection, analysis, and management. Finally, I explore the future of open source. Ultimately, Naquin's commentary illustrates how the post-9/11 open source debate reflects the paradox created when speakers attempt to fuse the concepts of secrecy and openness.[14] Paradoxes delimit options for thought and action, ''particularly if there is

little awareness of what is happening or if [stakeholders] are unable to comment on it."[15] Therefore, this exploration of the paradox of open source is useful for envisioning and developing the nation's intelligence capabilities.

INSTITUTIONAL CHANGE

Institutions are sets of beliefs coupled with observable and recurring practices.[16] For example, the institution of medical practice entails beliefs about what constitutes "good" or "bad" medical care, as well as routine and observable therapies and technical applications (e.g., a "check up" or an x-ray). Major institutions, such as the legal system, government, and education, exist partly within people's minds as cognitive frameworks for how to get things done. These institutions are also manifested in formal documents that guide action and can be archived for reference by institutional members. U.S. intelligence can be considered an institution because it is characterized by routinized and observable practices (e.g., collection and analysis), beliefs about the nature and uses of intelligence (e.g., "decision advantage"), and associated formal texts (e.g., President's daily briefs [PDBs], National Intelligence Estimates [NIEs], policies, and directives).

Institutions change slowly, and multiple social-scientific disciplines have attempted to describe and explain why and how they do.[17] One perspective maintains that institutions depend foremost on the relative distribution of scarce financial resources. For example, Richard S. Conley describes how President George W. Bush was able to leave an indelible imprint on the shape of counterterrorism programs due to his ability to shift budget priorities despite congressional inertia or resistance.[18] In this "materialist" vein, Naquin notes that while officials' respect for, and understanding of, open source have improved within the IC, financial constraints continue to hinder its development:

> Compared to seven years ago, when the OSC stood up, I believe there is increased respect for the contributions open sources make to the broader intelligence enterprise and general stakeholder [i.e., DNI] satisfaction that the Open Source investments made in the 2006–2009 period have provided a good return. Furthermore, I believe there has been progress in helping stakeholders understand that effective Open Source exploitation requires discipline, methodologies, and tradecraft not easily or widely available. On the other hand, we have not made great progress toward an IC-wide Open Source Enterprise. First, economic realities continue to limit individual agencies' investments in Open Source, and with more austere budgets on the horizon, I would be surprised if Open Source-specific investments competed well. Second, if the prevailing school of thought is that the true value of open sources depends on how well they are integrated with more clandestinely

> acquired material, there might be less interest in building a distinct Open Source Enterprise. In an era of tight budgets, and despite the potential economies of scale, no one agency is going to be keen to resource an IC-wide Open Source program unless there is a greater commitment among individual agencies to build their own capabilities and contribute, in turn, to the enterprise.

Naquin's comment bolsters intelligence scholar Amy Zegart's claim that the nature of bureaucratic organizations, the ability of bureaucrats to protect their turf, and the fragmented structure of the U.S. federal government tend to stymie significant IC reform.[19] The lack of financial commitment among some intelligence officials reinforces open source's persistent status as a subordinate intelligence discipline. According to Naquin, ''One could certainly argue that the creation of a DNI center represents the institutionalization of open source in the IC, but as of February 2012, most IC institutions had not yet altered their thinking on open sources in a programmatic sense, e.g., as an area worthy of discrete attention.''

One way to explain officials' lack of commitment to open source is to examine its symbolic meaning. From this perspective, institutional change relies less upon financial resources and more upon the skill of ''institutional entrepreneurs'' or ''change agents'' to influence the production, dissemination, and embedding of formal and informal texts that give rise to new meanings and institutional arrangements—and, ultimately, new budget priorities.[20] This perspective maintains that institutional ''entrepreneurs'' who are skilled at creating, disseminating, and embedding influential texts tend to exert more influence than those who are not.[21] Naquin acknowledges this symbolic dimension of institutional change when he states:

> When OSC stood up on November 1, 2005, we had to address a perception among many outside CIA that OSC would be too CIA-centric, a view with roots in the reductions to FBIS in the late 1990s but also because OSC remained organizationally in CIA. Strategically and tactically, we had to demonstrate value to organizations outside CIA if we were going to be accepted as an IC center beyond disseminating OSC's products USG-wide. We also had to be more open to expertise and capabilities outside OSC, acknowledging that transitioning from a media monitoring organization to a true *Open Source* Center involved skills, data, and perspective we did not have on staff. To this end, we became more extroverted.

Part of that ''extroversion'' involved participating in two open source conferences held in Washington, DC, in 2007 and 2008. Funding for both conferences was provided by the DNI. As the first IC conferences open to the general public in the history of the institution, their objective was to help legitimate open source as both a contributor to, and a unique form of

intelligence within, organizations that had historically been reluctant to apply that moniker to public information. Naquin states:

> From my perspective, the DNI-sponsored conferences in 2007 and 2008 (1) signaled publicly that the Intelligence Community was indeed taking Open Source seriously; (2) highlighted efforts in the U.S. Government and private sector that might have otherwise gone unnoticed or unappreciated even by people in the Intelligence Community; and (3) brought together a variety of people and organizations to promote the concept of an ''Open Source Enterprise.''

Despite the DNI's aggressive promotion of open source among key stakeholders, Naquin suggests that the conferences did little to fundamentally revise underlying institutional logics and commitments:

> Although there has long been talk that Open Source can provide a 'safety net' and might be 'good enough' on its own for certain issues, I never observed a willingness during high-level budget discussions to trade even small pieces of more traditional intelligence capabilities for investment in more comprehensive collection and analysis of open sources. It's not that such a scenario is inconceivable; it would just represent a major paradigm shift for the Intelligence Community. Such a trade would be a bellwether in the evolution of Open Source as an intelligence discipline.

Such a ''paradigm shift'' requires altering the symbolic meaning of open source, elevating its perceived value to the level of other intelligence disciplines through multiple, diverse, and sustained forms of ''institutional work.''[22] Despite evidence that such symbolic parity appears unlikely to occur anytime soon, Naquin suggests that IC managers can, at least theoretically, help bring it about. Specifically, for Naquin, the heart of the programmatic issue with open source lies with the general perception (or ''vision'') in IC organizations of their ''core'' missions. This, Naquin suggests, is where the institutional preference for secrecy is most acutely felt. Many IC senior managers would probably assert that their organization's ''core mission'' centers on clandestine collection, all-source analysis, covert action, or some other activity that emphasizes secrecy. But, informational activities such as clandestine collection and all-source analysis are better conceptualized as means or capabilities supporting the broader mission of the IC as a whole, which involves providing useful information to those who make and execute national security policy. If this broader conception of ''mission'' actually held sway across official and unofficial texts, as well as in everyday organizational processes and member interactions, then the value of open source's symbolic currency could rise. In absence of such institutional transformation, however, open source will continue to require a ''functional manager'' to more-or-less shoehorn open source into the plans, policies, and practices of IC

organizations. Officials are thus unlikely to soon consider the ways that open source's symbolic meaning might be radically altered in ways that destabilize deeply embedded IC beliefs and practices. The result may be that austere budgets will constrain the development of open source capabilities as rationally self-interested officials continue to resort to institutional protection of what they perceive to be "core" intelligence capabilities.

The material/symbolic dialectic is closely related to another: structure/agency. In Anthony Giddens's structuration theory, "structure" is regarded as stable rules and resources that guide routinized social interaction. Structure makes it possible for the seventeen formal members of the IC, scores of related government organizations and departments, and hundreds of private and non-governmental partners to conduct and coordinate similar intelligence practices across time and space.[23] When institutional structures become taken-for-granted and habitual, members' ability to recognize and alter ineffective or outmoded practices may become constrained.[24] The term "agency" thus refers not only to an organization but to people's capability to perpetrate events or to "make a difference."[25] Yet, agency is always reciprocally related to structure.[26] For Naquin, open source structures are still relatively new and evolving, therefore the intentions and actions of key figures remain critical:

> In my last couple of years, I became concerned that the lack of a designated Open Source champion or sponsor at the agency level would hamstring further progress if not undo the gains we had made both in OSC and the Community at large. I believed it was essential that the DNI have a 'point person' for Open Source at the program (or agency) level—someone he held accountable for the state of Open Source in the IC as he did for HUMINT, SIGINT, GEOINT, and MASINT. We had the good fortune in my last year to have both a DNI and DCIA who were knowledgeable and appreciative of the contributions of Open Source and understood the importance of a coherent IC-wide approach. This led to the DNI's appointing the DCIA as 'functional manager' for Community Open Source in mid-2012. This was an important step toward validation of Open Source as a discipline.

Naquin also identifies certain figures as either promoting or impeding post-9/11 open source reforms:

> The only difference [from similar open source reforms in the 1990s], post-9/11, was that we had a Principal Deputy Director for National Intelligence—Michael Hayden—who took the 'Second Renaissance' [of open source] seriously. I believe had he not been in place and then had not moved to become CIA director, OSC would not exist today, or would exist in much different form. As for other IC agencies, I experienced little energy for an enterprise approach to open source

> exploitation post-9/11. . . . It [also] seemed to us on more than one occasion that people who had never worked in Open Source were taken more seriously on matters of Open Source exploitation, even though they knew very little about what was being done or the resource and requirements environment in which we worked.

While intelligence scholars often focus on structural reforms,[27] Naquin's comments underscore that the actions of key individuals are crucial in promoting or impeding institutional change. Post-9/11 structural reforms have aided open source's institutionalization within the IC, but stakeholders would do well to also identify the specific figures likely to influence the changes to come. In sum, privileging material (read ''financial'' or ''technological'') and structural factors within the open source arena is not ''wrong,'' but recognizing and strategically managing the role of symbolism and agency may help open source stakeholders identify new and useful ways to achieve their objectives.

OPEN SOURCE PRACTICE

Three tensions characterize the practice of open source occurring in formal organizational settings. In contrast to the factors that influence institutional change, the focus here is on workplace activities and interactions that are, to some degree, ''transferable, teachable, transmittable or reproducible.''[28] First, open source practice involves the collection and analysis of publicly available information. In his recent volume on open source, Anthony Olcott concluded that the main benefit of the ever-burgeoning supply of open source information is that it can help the nation build an ever-improving capacity to anticipate potentialities and deal with the consequences of events.[29] Olcott implied that the sheer volume of information should lead to better analysis and prediction. But Olcott also acknowledged that information is made meaningful only within a particular context; and Naquin emphasizes the importance of context:

> If one looks at what's publicly available today compared to five years ago, one cannot help but infer the potential for greater intelligence value, and what will be available five years hence is likely to eclipse what is available today. Still, more data does not necessarily equate to better information, let alone better intelligence. Context is everything. I agree with [Olcott] that the odds to assess and anticipate events from publicly available information are better, but only in the hands of people who can navigate these data successfully with the appropriate discipline and context.

Naquin warns stakeholders to guard against the allure of the ''technological fix''—the idea that the problems of open source collection and analysis,

created by the development and diffusion of new technologies, can be overcome with even more technology:

> 'Big data' is big in the USG [U.S. government], driven by the volume and variety of data now publicly available. Social media are a major driver, and the 'Arab Spring' served as a wake-up call. In general, though, the amount of data of potential intelligence value—and the digital incarnation of these data—has everyone talking about harnessing petabytes, exabytes, and so on. Fair enough, but I caution that we not overemphasize 'big data' as a technical challenge or believe that hiring an army of 'data scientists' will send us on our way to pressing F9 to predict the next social upheaval. While technology and greater statistical facility among those exploiting 'big data' might be necessary, they are far from sufficient. Anyone who has spent time analyzing foreign open sources, for example, knows that the key to insight is about 30% 'data navigation' and 70% knowing what, where, and how to seek. Developing methodologies for this 70% is at least as important. First, cultural and linguistic factors loom large not only in assessing the value of the data itself but in considering the social and communication dynamics under which these data are produced and shared. Second, analysts will have to be sufficiently grounded in the substance of their area of focus—not just expertise in the topic or political issue but in the relevant information (e.g., media/publishing) environments, socio-communication dynamics and infrastructure, and the various factors that affect not just what people say/publish but how they communicate. In short, 'big data' is not just crunching numbers. Technology and statistical analysis should allow us to organize haystacks better, but I believe we will still depend on substantive—and Open Source—experts to derive insight from those haystacks, let alone find any needles.

The tension between systematized, technology-enabled message processing versus human context and interpretation finds expression in the related tension between open source exceptionalism and integration. In other words, the path of open source's development hinges on whether stakeholders believe it is a unique and exceptional activity, or whether it is simply a commoditized input within established intelligence disciplines and processes. As Naquin cautioned:

> I believe Open Source is increasingly accepted as essential to the intelligence process, and social media and 'big data' are the latest drivers in raising its profile. Still, until the IC and national security community, in general, treat Open Source programmatically (i.e., as a discipline and not solely as a commodity), I'm afraid efforts will remain fragmented, and monitoring and assessing just how well the IC is doing in exploiting open sources will be difficult. . . . My experience is that most in the Intelligence Community see the value of open

> sources in how these sources facilitate a specific, and usually unique, intelligence mission. This perspective is understandable but fails to take into account factors like economies of scale and risk. First, in some cases it might not make sense for several different agencies to buy or contract for essentially the same work or data. Second, there is increasingly an issue of 'quality control' when it comes to the collection and analysis of publicly available material. One reason I believe some say they cannot 'trust' open sources' reliability is because they have no means or methodology to vet them. Methodologies and tradecraft are just as important in vetting and forming open source-based assessments as they are in forming more clandestine-oriented assessments—and they do, in fact, exist. A center like OSC potentially offers a tremendous service by helping multiple agencies realize economies of scale and—through training and standards—reduce risk that might result from underdeveloped methodologies or tradecraft.

Although Naquin identifies methodological rigor and economies of scale as key benefits of the OSC, many organizations continue to pursue ''outside'' open source capabilities from private-sector vendors. This tension may stem, in part, from the OSC's original mandate, which involved focusing on services that complemented and strengthened component-specific or agency-specific open source efforts. Then-DCIA Michael V. Hayden emphasized in 2005 that the OSC would not serve as a ''one-stop shop'' for open source.[30] Within these parameters, Naquin noted, OSC needed to find its niche:

> For the last several years, we observed an increasing confluence of private sector and Intelligence Community interests in leveraging open sources. In some cases, our interests might coincide, for example, in assessing the stability or policies of a foreign government or tracking the path of an epidemic. In other cases, we might be able to use the same approaches and methodologies to answer different questions. In either scenario, we were finding the private sector to possess expertise, technology, or access that would either be beyond our capability or cost too much to replicate. We increasingly saw opportunities to leverage these capabilities for new intelligence benefit and began to develop an operating—or business—model based on fostering partnerships with those who possessed unique capabilities. The concurrent challenge, however, was 'quality assurance.' In OSC, we used the term 'trusted interlocutor' as a role we saw ourselves playing more in the future as we engaged with partners both inside and outside the US Government. We found ourselves expanding into areas where someone in the private sector found it commercially advantageous to establish a capability, and then took on the role of broker to transition that capability safely within an intelligence context—a role we saw as unique and important. . . . I believe the relationship between government agencies and private sector contractors on open source is healthy. Speaking for OSC, we were

> outsourcing more and more work that did not require clearances, and even some that did. In fact, most new capabilities (products and services) we pursued since becoming a center entailed some type of partnership or contracting agreement. In most other IC components, I would venture to say that the vast majority of open source-related work is done by contractors. This can be good and bad, however. A rule of thumb is that an organization should not outsource work in which it has no competency (to be able to provide quality assurance). Those agencies that depend entirely on contractors for their open source work might not be in a position to judge the quality of what they're getting.

In sum, tensions between and among materiality/symbolism, structure/agency, message processing/human context, exceptionalism/integration, and internal/external production characterize the post-9/11 open source debate. Understanding how the IC has coped with the abundance of publicly available information necessarily leads to a discussion of one or more of these tensions. Emphasizing one tension does not negate the others; privileging one term within each dialectical pair does not render the other irrelevant. All perspectives necessarily prioritize some issues and downplay others. The point here is that adequately anticipating the trajectory of open source developments requires awareness of all of them.

THE FUTURE OF OPEN SOURCE

While some of the tensions described here stem from institutional design, their common source can be traced, in part, to the paradox created when speakers attempt to conceptually fuse openness and secrecy. From one perspective, secrecy is what makes intelligence a unique category of information.[31] Therefore, a paradox is created when conflating public information and the secrets that constitute the conceptual basis of intelligence. In a paradoxical situation, when speakers pursue one goal (equating open source and intelligence), their pursuit of a competing goal (defining open source as conceptually distinct from intelligence) is undermined. One way to manage a paradoxical dilemma is to establish a hierarchy among the terms. For example, in its *Final Report*, the 9/11 Commission called for an "Open Source Agency" residing outside the CIA.[32] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, however, urged the "creation of an Open Source Directorate at the CIA."[33] Some have interpreted the 9/11 Commission's proposal as privileging openness and underscoring a need for more IC transparency and accountability.[34] The WMD Commission's proposal maintained the institutional status quo, leaving the ideal of openness subordinate to secrecy. These competing proposals had followed a steady stream of diverse recommendations from officials, scholars, and commentators on how to best collect, manage, and exploit open sources in

order to protect the United States and advance its security interests.[35] The WMD Commission's proposal was ultimately selected as the basis for the OSC. While calls for an open source agency residing outside the IC persist, conceptually speaking, a public open source agency seems to undermine both the established institutional hierarchy and the assumed purpose of the IC, namely, to generate actionable intelligence that policymakers can use to improve U.S. security and/or advance national interests. Naquin explains:

> One of the ironies of working in Open Source Intelligence is that the better we got, the less we could say about our successes. We did enjoy several notable successes that garnered kudos from leaders and stakeholders both inside and outside the Intelligence Community, but given the nature of these stories I cannot be specific. At a macro level, however, I believe our investment in an Emerging Media Group in 2007 positioned OSC for the explosion in social media, first with the 'green revolution' in Iran in June 2009 and later with the 'Arab Spring' in early 2011. I also believe our investments in IT helped a modestly sized organization harness and share a much greater volume and variety of information throughout the US Government than was possible a few years earlier.

Naquin's comments highlight the paradox generated when the imperative to protect intelligence sources and methods collides with the ideals of openness, transparency, and accountability. I have argued elsewhere that the IC's institutional preference for secrecy diminishes the democratic potential of open source. For example, the State Department in December 2012 announced a contest that "aims to harness the ingenuity of American and Russian citizens to think creatively about innovative ways to use open source information and communication technologies (ICTs) for arms control verification, compliance monitoring, and monitoring of sensitive facilities."[36] While such open source initiatives are rare, they nevertheless illustrate its democratic potential. Naquin, however, suggests that such initiatives are unlikely to become a routine practice within the IC:

> One way to look at the 'logic of secrecy' is to presume that if I earn an intelligence advantage, it would not be wise of me to undermine my position by sharing the information that gave me that advantage. If one accepts that premise, then it should make no difference whether I obtained that information through clandestine means or from publicly available sources. In fact, those in the Open Source domain are doing their jobs well if they provide information that is deemed valuable enough to protect. That said, somewhere along the value chain of creating intelligence that is worthy of protection there is usually information ('raw material') that is indeed more shareable. Our goal in OSC was to make as much of the material—and resulting products—at our disposal available to as wide an audience as possible, but at the point

> we needed to protect methods, advantage, or customer, we treated our work product just as any intelligence component would.

Nevertheless, Naquin acknowledges the potential upshot of the (partial) democratization of open source:

> Although I am certain there would be legal and resourcing issues to tackle as the 'network' expanded beyond agency and government domains, as long as there is a recognized center or headquarters to set and uphold standards, operating procedures, the rule of law, and other matters of governance, I believe a more distributed business model for Open Source can be effective in supporting national security.

A CONSEQUENTIAL DEVELOPMENT

The tensions discussed herein can be traced, in part, to the paradox created when attempting to conceptually fuse openness and secrecy. Such tensions are not unique to open source; they parallel major themes within organizational theory writ large. However, since 2005, the five tensions discussed herein have overwhelmingly and consistently appeared within the speech and writing of open source stakeholders, and they similarly exemplify the major themes of Naquin's commentary. Naquin concludes:

> In general, throughout the decade we saw a growing need to address 'mysteries and puzzles,' as much as individual secrets, and we believed competent exploitation of publicly available material could shed increasing light. This opportunity is both a boon and challenge to intelligence professionals, however: With greater access and potential to collect one's own intelligence comes the potential to do so badly.

The ''boons'' and ''challenges'' that characterize the post-9/11 open source debate have now been largely clarified. Some open source stakeholders may choose to downplay, suppress, or ignore one term within each dialectical pair, that is, assert that openness should trump secrecy,[37] or that secrecy should trump openness;[38] however, the underlying tensions are unlikely to be fully or forever resolved.[39] What is needed is management of the dialectic in ways that promote the nation's most cherished values and purposes, rather than a struggle to ''fix'' the meaning of open source in particular ways for narrow bureaucratic ends or economic interests.

From 2005 to 2012, Douglas Naquin managed those tensions and was personally critical to the development of open source policies, programs, and practices. Irrespective of how stakeholders ultimately judge the open source enterprise, its development has been demonstrably complex, contentious, and consequential.

REFERENCES

[1] Katherine Schrader, ''New U.S. Intel Center Studies Free Secrets,'' Associated Press, 8 November 2005.

[2] Establishment of the DNI Open Source Center, ''DNI and D/CIA Announce Establishment of the DNI Open Source Center,'' CIA Press Releases and Statements, 8 November 2005, at https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html, para. 2.

[3] Katherine Schrader, ''New U.S. Intel Center,'' para. 1.

[4] *Ibid*., para. 2.

[5] Open Source Center, 2008, ''Open Source Center,'' at https://www.opensource.gov

[6] *Ibid*.

[7] Kimberly Dozier, ''CIA Following Twitter, Facebook,'' Associated Press, 4 November 2011, para. 2.

[8] *Ibid*., para. 11.

[9] *Ibid*., paras. 15–22.

[10] See Hamilton Bean, ''The DNI's Open Source Center: An Organizational Communication Perspective,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 2, Summer 2007, pp. 240–257; Glenn P. Hastedt, ''Intelligence Estimates: NIEs vs. the Open Press in the 1958 China Strait Crisis,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 23, No. 1, Spring 2009, pp. 104–132; Arthur S. Hulnick, ''The Downside of Open Source Intelligence,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 15, No. 4, Winter 2002–2003, pp. 565–579; G. Mert McGill, ''OSCINT and the Private Information Sector,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 7, No. 4, Winter 1994–1995, pp. 435–443; Robert W. Pringle, ''The Limits of OSINT: Diagnosing the Soviet Media, 1985–1989,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 16, No. 2, Summer 2003, pp. 280–289; Robert David Steele, ''A Critical Evaluation of U.S. National Intelligence,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 6. No. 2, Summer 1993, pp. 173–193; Robert David Steele, ''Reinventing Intelligence: Holy Grail or Mission Impossible?'' *International Journal of Intelligence and CounterIntelligence*, Vol. 7, No. 2, Summer 1994, pp. 199–203; Robert David Steele, ''The Importance of Open Source Intelligence to the Military,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 8, No. 4, Winter 1995–1996, pp. 457–470; Robert David Steele, ''The Open Source Program: Missing in Action,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 21, No. 3, Fall 2008, pp. 609–619; Robert David Steele, ''Shedding Light on the Secret World,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 25, No. 3, Fall 2012, pp. 634–638; Michael A. Turner, ''Open Sourcing the Drug War,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 12, No. 4, Winter 1999–2000, pp. 103–108.

[11] Readers seeking prescriptive or normative assessments of open source should consult these volumes: Edward J. Appel, *Internet Searches for Vetting*

Investigations and Open-Source Intelligence (Boca Raton, FL: CRC Press, 2011); Michael Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (CreateSpace Independent Publishing Platform, 2013); Anthony Olcott, *Open Source Intelligence in a Networked World* (London and New York: Continuum Books, 2012); Robert David Steele, *The Open-Source Everything Manifesto: Transparency, Truth, and Trust* (Berkeley, CA: Evolver Editions, 2012); Selma Tekir, *Open Source Intelligence Analysis* (Saarbrücken: VDM Verlag, 2009); Uffe Kock Wiil, *Counterterrorism and Open Source Intelligence* (Vienna: Springer-Verlag, 2011).

[12] In December 2012, Douglas J. Naquin agreed to provide written answers to a set of generalized questions from me about the development of the IC's open source enterprise.

[13] Katherine Schrader, ''New U.S. Intel Center Studies Free Secrets,'' para. 11; additionally, see Richard A. Best Jr. and Alfred Cumming, ''Open Source Intelligence (OSINT): Issues for Congress,'' Congressional Research Service, 2007; Wyn Q. Bowen, ''Open Source Intelligence and Nuclear Safeguards,'' in *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence*, Robert Dover and Michael S. Goodman, eds. (New York: Columbia University Press, 2009), pp. 91–104; Herman L. Croom, ''The Exploitation of Foreign Open Sources,'' *Studies in Intelligence*, Vol. 13, Summer 1969, pp. 129–136; J. F. Holden-Rhodes, *Sharing the Secrets: Open Source Intelligence and the War on Drugs* (Albuquerque, NM: The University of New Mexico Printing Services, 1994); Mark M. Lowenthal, ''Open Source Intelligence: New Myths, New Realities,'' *Intelligencer*, Vol. 10, No. 1, February 1999, pp. 7–9; Ronald Marks, ''Twittering Intelligence,'' Open Source Intelligence Forum, February 2009, at http://www.osif.us/articlesofinterest.html, accessed 21 November 2010; Stephen C. Mercado, ''Sailing the Sea of OSINT in the Information Age,'' *Studies in Intelligence*, Vol. 48, No. 3, 2004; Stephen C. Mercado, ''Reexamining the Distinction Between Open Information and Secrets,'' *Studies in Intelligence*, Vol. 49, No. 2, 2005; Paul F. Wallner, ''Open Sources and the Intelligence Community: Myths and Realities,'' *American Intelligence Journal*, Spring/Summer 1993, pp. 19–24.

[14] Anthony Olcott in *Open Source Intelligence in a Networked World* discussed the ''paradoxes of choice,'' i.e., while more information is seemingly always desirable, it creates problems in terms of choosing among alternatives, as well as the timeliness and quality of decision-making. The paradox discussed herein differs from Olcott's in that the focus here is on secrecy and openness as competing values within U.S. national security affairs.

[15] Cynthia Stohl and George Cheney, ''Participatory Processes/Paradoxical Practices: Participation and the Dilemmas of Organizational Democracy,'' *Management Communication Quarterly*, Vol. 14, No. 3, February 2001, p. 352.

[16] John C. Lammers and Joshua B. Barbour, ''An Institutional Theory of Organizational Communication,'' *Communication Theory*, Vol. 16, 2006, pp. 1–22.

[17] Paul J. DiMaggio and Walter W. Powell, *The New Institutionalism in Organizational Analysis* (Chicago: University of Chicago Press, 1991); Douglass C. North,

Institutions, Institutional Change, and Economic Performance (Cambridge, UK: Cambridge University Press, 1990); M. Tina Dacin, Jerry Goodstein, and W. Richard Scott, ''Institutional Theory and Institutional Change: Introduction to the Special Research Forum,'' *Academy of Management Journal*, Vol. 45, 2002, pp. 45–57.

[18] Richard S. Conley, ''Reform, Reorganization, and the Renaissance of the Managerial Presidency: The Impact of 9/11 on the Executive Establishment,'' *Politics & Policy*, Vol. 34, No. 2, June 2006, pp. 304–342.

[19] Amy B. Zegart, ''An Empirical Analysis of Failed Intelligence Reforms Before September 11,'' *Political Science Quarterly*, Vol. 121, 2006, pp. 33–60.

[20] Nelson Phillips, Thomas B. Lawrence, and Cynthia Hardy, ''Discourse and Institutions,'' *Academy of Management Review*, Vol. 29, 2004, pp. 635–652.

[21] Thomas B. Lawrence and Roy Suddaby, ''Institutions and Institutional Work,'' in *The Sage Handbook of Organization Studies*, 2nd ed., Stewart R. Clegg, Cynthia Hardy, Thomas B. Lawrence and Walter R. Nord, eds. (London: Sage, 2006) pp. 215–245.

[22] See Hamilton Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence* (Santa Barbara, CA: Praeger, 2011); Thomas B. Lawrence and Roy Suddaby, ''Institutions and Institutional Work''; Markus Perkmann and Andre Spicer, ''How are Management Fashions Institutionalized? The Role of Institutional Work,'' *Human Relations*, Vol. 61, No. 6, 2008, pp. 811–844.

[23] Anthony Giddens, *The Constitution of Society: An Outline of the Theory of Structuration* (Berkeley, CA: University of California Press, 1984).

[24] Stephen R. Barley, ''Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments,'' *Administrative Science Quarterly*, Vol. 31, No. 1, 1986, pp. 78–108.

[25] Francois Cooren, ''Textual Agency: How Texts do Things in Organizational Settings,'' *Organization*, Vol. 11, 2004, p. 375.

[26] Stephen R. Barley and P. S. Tolbert, ''Institutionalization and Structuration: Studying the Links between Action and Institution,'' *Organization Studies*, Vol. 19, 1997, pp. 93–117.

[27] Thomas H. Hammond, ''Intelligence Organizations and the Organization of Intelligence,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 23, No. 4, Winter 2010–2011, pp. 680–724; for a critique, see Joshua Rovner and Austin Long, ''The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 18, No. 4, Winter 2005–2006, pp. 609–637.

[28] Gessica Corradi, Silvia Gherardi, and Luca Verzelloni, ''Through the Practice Lens: Where is the Bandwagon of Practice Based Studies Heading?'' *Management Learning*, Vol. 41, No. 3, 2010, p. 267.

[29] Anthony Olcott, *Open Source Intelligence in a Networked World.*

[30] Hamilton Bean, ''The DNI's Open Source Center.''

[31] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2006).

[32] National Commission on Terrorist Attacks upon the United States. (2004). *Final Report*, at http://www.9-11commission.gov/, accessed 4 August 2008.

[33] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005). Report to the President, at http://www.wmd.gov/report, accessed 3 August 2008.

[34] Hamilton Bean, *No More Secrets*; Robert David Steele, "Shedding Light on the Secret World."

[35] United States Congress, House of Representatives, Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "Using Open-Source Information Effectively: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment," 109th Congress, 1st Session, 21 June 2005.

[36] James Martin Center for Nonproliferation Studies "To Boldly Go: Harnessing Open Source Technologies for International Arms Control," at http://cns.miis.edu/stories/121206_open_source_esssay_contest.htm, accessed 6 December 2012.

[37] Robert David Steele, "Shedding Light on the Secret World."

[38] Jennifer E. Sims, "Defending Adaptive Realism: Intelligence Theory Comes of Age," in *Intelligence Theory: Key Questions and Debates*, Peter Gill, ed. (New York: Routledge, 2009), p. 154.

[39] Charles Conrad, "Organizational Discourse Analysis: Avoiding the Determinism-Voluntarism Trap," *Organization*, Vol. 11, 2004, pp. 427–439.