No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence

Hamilton Bean, (Santa Barbara CA: Praeger, 2011), 218 pp, bibliography, index.

Reviewed by Anthony Olcott

Author Hamilton Bean never really delivers on what is promised in the title of this book. He neither examines what "open source information" might mean in relationship to intelligence, nor does he explain what he means by "No More Secrets." Is this a description of information abundance? An exhortation to cultural change within the Intelligence Community (IC)? Something else?

Bean writes that for a time he worked at a small contracting company that provided what was basically a clipping service to its mostly military clients by culling newspapers and other open sources for materials the company presumed met its customers' open source intelligence (OSINT) requirements. After the company was sold, Bean returned to school, earned a PhD in communications, and turned to more academic pursuits, such as writing this book.

After a short, even perfunctory, history of the Foreign Broadcast Information Service (FBIS), most of it taken from *Studies in Intelligence* articles or Joseph Roop's history posted on cia.gov,[a] the bulk of Bean's book is an examination of the period between the 9/11 attacks in 2001 and the Director of National Intelligence's (DNI) Open Source Conference in 2008, a period that included the conversion of FBIS into the DNI's Open Source Center (OSC).

As Bean explains, there was considerable pressure then to get the IC to use more open source information–the 9/11 Commission had called for the creation of an "Open Source Agency" equal to the CIA, and the WMD Commission later (2005) urged the creation of an Open Source Directorate within CIA. What resulted instead was the National Open Source Enterprise (known by the unhappy acronym NOSE) within the DNI. The DNI continued to oversee OSC, which became part of the NOSE but remained little changed from its predecessor.

Bean uses what he calls "discourse analysis" to examine the process by which OSC came to be, studying not the substance of OSINT, but rather the various ways participants in the process talked or wrote about it. Viewed in an institutional framework, the primary challenge for the new organization was not how to make better use of the vast quantities of freely available information, but rather to find presentational ways to make the material more acceptable to the rest of the IC. One of these was to restrict the availability of its products. This, Bean asserts, played to IC values, which favor the secret over the open. In his words: "OSC may not necessarily require its current level of secrecy to operate effectively, but that secrecy encourages intelligence stakeholders to view OSC as legitimate." (43)

In Bean's view, the recipients of intelligence, "the customers," are more focused on the *form* in which they receive information than they are in its content or possible uses. The reason for this, he argues, is that intelligence has an

---

[a] https://www.cia/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/index.html

---

institutional dimension, marking those who receive it (just as it does those who produce it) as distinct from other people. The greatest challenge of open source information, in this view, is not the mind-boggling quantities of information or the complex epistemological issue of what part of that ocean of information will help answer particular questions, but rather how to preserve the "specialness" of intelligence when it is derived from sources that anyone can access.

Where that challenge shows most plainly, in Bean's view, is in the struggle over "information sharing." The ease with which unclassified materials may be shared is one of the major arguments usually given in favor of open source, but it is precisely the loss of exclusivity that makes users and practitioners reluctant to loosen their grip on information products. In Bean's account, the various contradictions and conflicts show most clearly in the Department of Homeland Security (DHS), which had a former head of intelligence and analysis, whom Bean described as having a "mind-set to stay on the dark side," as well as others who believed that material should go to "every cop on the street." (96) The pattern Bean describes is one of "officials…simply asserting the need for a culture of information sharing within and among federal, state, and local agencies" while "gloss[ing] over critical differences that influence stakeholders' perceptions and practices"

(96-97). The result is that many DHS units pay lip service to meet "the minimum standard [to] improve OSINT," mostly by contracting out open source collection to commercial providers while keeping the efforts "minimally resourced" (100), a practice that even the contractors characterize as "check the box" exercises. (99).

Unfortunately for his argument, Bean does not offer examples of how open source information might be better used. Arguably, this could be a product of Bean's willingness to take "intelligence" as something with a clear definition, which results in some way from the working out of the "intelligence cycle." Add more OSINT to collection, Bean seems to argue, and "analysis" will improve. However, even within that narrow definition of what open source information might add to the production of intelligence, Bean is convinced that institutional structures and cultural constraints are such that "institutional insecurity regarding the worth of open source and its status as a legitimate form of intelligence endures" (161).

In the end, this reviewer is left puzzled, though definitely intrigued. Are Bean's long paragraphs and jargon-filled prose simply a product of academic turgidity, or has he contrived to conceal a sly but ultimately quite damning argument about the place of OSINT in the IC?

❖ ❖ ❖