DIALOGUE

OPEN SOURCE EXPERIMENTS

What They Show About the Analyst’s Frustrations in Intelligence Communities

CHRISTOPHER KELTY
Rice U

GEORGE E MARCUS
UC Irvine

When the question of ethics emerges around the topic of intelligence gathering, security and spying, the first questions anthropologists usually pose are frequently similar to the following: Should the CIA fund my research? Should I answer their questions? Should I give them my research? Should I agree to secrecy? Good questions, no doubt, but are they the right ones? The AAA Commission on the Engagement of Anthropology with the US Security and Intelligence Communities intends to investigate another, perhaps more troubling question that precedes these concerns and changes the nature of the default ethical imperative. To wit: How does research (whether anthropological monograph or secret info from spies) gain traction and become influential within the defense and intelligence agencies of contemporary nations?

Research and Influence

Before we assume that our research will help or hurt, should we be wondering how—and more likely—if it will ever see the light of day at all? Even if the information is truly helpful—even if an anthropologist is ethically and professionally comfortable with assisting the worlds of classified and secret knowing, how likely is it that such information will have effect before it is filed?

It was a recent NYT Magazine article (December 3, 2006, by Clive Thompson) that raised this question most sharply: “In a world that is awash in information ... the meaning of intelligence is shifting.” The article, “Open-Source Spying,” reports on recent experiments in the intelligence community with what are known amongst the Internet digerati as Web 2.0 tools: blogs, wikis and “social software” that allow for large numbers of people to quickly post and communicate information in structured ways—the leading website—to do so is to abandon all hope of advancement. And secret here does not mean secure: the article points out that many spies distrust all electronic technologies, and prefer to keep their secrets in shoeboxes underneath their desks.

Order in Sharing and Secrecy

And yet, as the 9/11 Report made clear, the nature of intelligence today is in putting together little bits and pieces of highly disparate and diverse information—bits and pieces that mean nothing in itself but gain meaning when combined. The question is: how does this happen? How do bits become knowledge and knowledge becomes power? The best way to investigate this perhaps is to focus on the “security/intelligence” community—the people who build for having the right secrets at the right time. A spy who builds for having the right secrets in shoeboxes under their desks.

Reference

See Open Source on page 4
mean the Al Qaeda plotters themselves need only check their RSS readers daily to know just what intel Intel has on them.

By contrast, keeping the Intellipedia secret reduces its effectiveness—the more secret it is, the less effective it becomes—the limit case being the shoebox underneath the desk. Not only that, but the very problem of terrorism is that we don’t know who are terrorists and who are not—so we have no a priori way to exclude them except to be completely paranoid. Sharing and secrecy each produce their own kind of order. Or as the article puts it, “social software doesn’t work if people aren’t social.”

Thus there are conflicting demands: on one hand, a world awash with information and an emerging array of clever tools whose function is to manage that flood in an open and public manner (blogs, wikis, content management systems, RSS feeds, to say nothing of artificial intelligence projects to automate either the production or the consumption of information). On the other hand is an array of long-standing, sedentary practices and institutions (both academia and government) founded on an ideal of individual, autonomous and highly intelligent analysts who do the work of piecing together a story—whether that be a story of kinship and race, or a story of training camps and weapons-buying.

In the former, information has agency—and the Internet is its body; humans are condemned to “keep up” with it, “navigate” it, “surf” it or otherwise evolve strategies for solving problems and keeping afloat. In the latter, humans have agency, while information is conceived of as a kind of scarce good painstakingly collected like so many pottery sherds and cosmological diagrams.

Paradoxical Networks
What makes this opposition so interesting is that it is also operative for suspected evildoers—whether they be terrorists or Earth Firsters, social movement activists or hackers, Zapatistas or Hamas—they too are confronted with the question of what openness gets them, and what secrecy prevents. The Independent Media Centers, as Tish Stringer has shown, are ideologically and technologically devoted to maximum openness even as it puts them at risk of being discovered and targeted, either by right-wing fanatics or by the government. The Zapatistas—with their famous balacalava-wearing Subcommandante Marcos—play both sides: Marcos is a secret, but the network of supports and the flow of information and email about their movement is open and widespread.

Immediately after 9/11, Wired magazine published an issue whose cover declared “How to Win: Fighting the Network War” that showcased Rand researchers John Arquilla and David Ronfeldt in terms simultaneously present and nostalgic for the recently popped dot-com bubble. It was a kind of perfect connection between the dot-com digerati and the military strategists. But it turns out that not many people outside of Wired readers and Deleuze and Guattari fans have heard of these two guys—and certainly few if any of their ideas were implemented in the disastrous wars that followed 9/11.

Similarly, Thomas Barnett writes at length in “The Pentagon’s New Map” about how hard it is to get his ideas about re-configuring the strategy of the Pentagon to be heard outside of the lowest echelons. Whatever these ideas are—good or bad—just because they come with a .mil address or out of a PowerPoint presentation delivered to the CIA—it hardly means they are ideas with any traction. If we needed any further confirmation of this fact, the last five years of executive secrecy and deliberate refusal to accept any outside information should provide it. The structure of power in Washington—within the government bureaucracy—is somehow clearly at odds with the structure of knowledge production that Web 2.0 represents.

Christopher Kelty, Rice University, is the author of the forthcoming “Two Bits: the Cultural Significance of Free Software and the Internet.” George E Marcus is a member of the AAA Executive Board, a member of the AAA Commission on the Engagement of Anthropology with the US Security and Intelligence Communities and Chancellor’s Professor, Department of Anthropology, University of California-Irvine.