The New York Times
nytimes.com

December 3, 2006

Open-Source Spying

By CLIVE THOMPSON

When Matthew Burton arrived at the Defense Intelligence Agency in January 2003, he was excited about getting to his computer. Burton, who was then 22, had long been interested in international relations: he had studied Russian politics and interned at the U.S. consulate in Ukraine, helping to speed refugee applications of politically persecuted Ukrainians. But he was also a big high-tech geek fluent in Web-page engineering, and he spent hours every day chatting online with friends and updating his own blog. When he was hired by the D.I.A., he told me recently, his mind boggled at the futuristic, secret spy technology he would get to play with: search engines that can read minds, he figured. Desktop video conferencing with colleagues around the world. If the everyday Internet was so awesome, just imagine how much better the spy tools would be.

But when he got to his cubicle, his high-tech dreams collapsed. “The reality,” he later wrote ruefully, “was a colossal letdown.”

The spy agencies were saddled with technology that might have seemed cutting edge in 1995. When he went onto Intelink — the spy agencies’ secure internal computer network — the search engines were a pale shadow of Google, flooding him with thousands of useless results. If Burton wanted to find an expert to answer a question, the personnel directories were of no help. Worse, instant messaging with colleagues, his favorite way to hack out a problem, was impossible: every three-letter agency — from the Central Intelligence Agency to the National Security Agency to army commands — used different discussion groups and chat applications that couldn’t connect to one another. In a community of secret agents supposedly devoted to quickly amassing information, nobody had even a simple blog — that ubiquitous tool for broadly distributing your thoughts.

Something had gone horribly awry, Burton realized. Theoretically, the intelligence world ought to revolve around information sharing. If F.B.I. agents discover that Al Qaeda fund-raising is going on in Brooklyn, C.I.A. agents in Europe ought to be able to know that instantly. The Internet flourished under the credo that information wants to be free; the agencies, however, had created their online networks specifically to keep secrets safe, locked away so only a few could see them. This control over the flow of information, as the 9/11 Commission noted in its final report, was a crucial reason American intelligence agencies failed to prevent those attacks. All the clues were there — Al Qaeda associates studying aviation in Arizona, the flight student Zacarias Moussaoui arrested in Minnesota, surveillance of a Qaeda plotting session in Malaysia — but none of the agents knew about the existence of the other evidence. The report concluded that the agencies failed to “connect the dots.”

By way of contrast, every night when Burton went home, he was reminded of how good the everyday

Internet had become at connecting dots. “Web 2.0” technologies that encourage people to share information — blogs, photo-posting sites like Flickr or the reader-generated encyclopedia Wikipedia — often made it easier to collaborate with others. When the Orange Revolution erupted in Ukraine in late 2004, Burton went to Technorati, a search engine that scours the “blogosphere,” to find the most authoritative blog postings on the subject. Within minutes, he had found sites with insightful commentary from American expatriates who were talking to locals in Kiev and on-the-fly debates among political analysts over what it meant. Because he and his fellow spies were stuck with outdated technology, they had no comparable way to cooperate — to find colleagues with common interests and brainstorm online.

Burton, who has since left the D.I.A., is not alone in his concern. Indeed, throughout the intelligence community, spies are beginning to wonder why their technology has fallen so far behind — and talk among themselves about how to catch up. Some of the country’s most senior intelligence thinkers have joined the discussion, and surprisingly, many of them believe the answer may lie in the interactive tools the world’s teenagers are using to pass around YouTube videos and bicker online about their favorite bands. Billions of dollars’ worth of ultrasecret data networks couldn’t help spies piece together the clues to the worst terrorist plot ever. So perhaps, they argue, it’ s time to try something radically different. Could blogs and wikis prevent the next 9/11?

The job of an analyst used to be much more stable — even sedate. In the ’70s and ’80s, during the cold war, an intelligence analyst would show up for work at the C.I.A.’s headquarters in Langley, Va., or at the National Security Agency compound in Fort Meade, Md., and face a mess of paper. All day long, tips, memos and reports from field agents would arrive: cables from a covert-ops spy in Moscow describing a secret Soviet meeting, or perhaps fresh pictures of a missile silo. An analyst’s job was to take these raw pieces of intelligence and find patterns in the noise. In a crisis, his superiors might need a quick explanation of current events to pass on to their agency heads or to Congress. But mostly he was expected to perform long-term “strategic analysis” — to detect entirely new threats that were still forming.

And during the cold war, threats formed slowly. The Soviet Union was a ponderous bureaucracy that moved at the glacial speed of the five-year plan. Analysts studied the emergence of new tanks and missiles, pieces of hardware that took years to develop. One year, an analyst might report that the keel for a Soviet nuclear submarine had been laid; a few years later, a follow-up report would describe the submarine’s completion; even more years later, a final report would detail the sea trials. Writing reports was thus a leisurely affair, taking weeks or months; thousands of copies were printed up and distributed via interoffice mail. If an analyst’s report impressed his superiors, they’d pass it on to their superiors, and they to theirs — until, if the analyst was very lucky, it landed eventually in the president’s inner circle. But this sort of career achievement was rare. Of the thousands of analyst reports produced each year, the majority sat quietly gathering dust on agency shelves, unread by anyone.

Analysts also did not worry about anything other than their corners of the world. Russia experts focused on Russia, Nicaragua ones on Nicaragua. Even after the cold war ended, the major spy agencies divided up the world: the F.B.I. analyzed domestic crime, the C.I.A. collected intelligence internationally and military spy agencies, like the National Security Agency and National Geospatial-Intelligence Agency, evaluated threats to the national defense. If an analyst requested information from another agency, that request traveled through elaborate formal channels. The walls between the agencies were partly a matter of law. The charters

of the C.I.A. and the defense intelligence agencies prohibited them from spying on American citizens, under the logic that the intrusive tactics needed to investigate foreign threats would violate constitutional rights if applied at home. The F.B.I. even had an internal separation: agents investigating terrorist activity would not share information with those investigating crimes, worried that secrets gleaned from tailing Al Qaeda operatives might wind up publicly exposed in a criminal trial.

Then on Sept. 12, 2001, analysts showed up at their desks and faced a radically altered job. Islamist terrorists, as 9/11 proved, behaved utterly unlike the Soviet Union. They were rapid-moving, transnational and cellular. A corner-store burglar in L.A. might turn out to be a Qaeda sympathizer raising money for a plot being organized overseas. An imam in suburban Detroit could be recruiting local youths to send to the Sudan for paramilitary training. Al Qaeda operatives organized their plots in a hivelike fashion, with collaborators from Afghanistan to London using e-mail, instant messaging and Yahoo groups; rarely did a single mastermind run the show. To disrupt these new plots, some intelligence officials concluded, American agents and analysts would need to cooperate just as fluidly — trading tips quickly among agents and agencies. Following the usual chain of command could be fatal. “To fight a network like Al Qaeda, you need to behave like a network,” John Arquilla, the influential professor of defense at the Naval Postgraduate School, told me.

It was a fine vision. But analysts were saddled with technology that was designed in the cold war. They now at least had computers, and intelligence arrived as electronic messages instead of paper memos. But their computers still communicated almost exclusively with people inside their agencies. When the intelligence services were computerized in the ’90s, they had digitally replicated their cold-war divisions — each one building a multimillion-dollar system that allowed the agency to share information internally but not readily with anyone outside.

The computer systems were designed to be “air gapped.” The F.B.I. terminals were connected to one another — but not to the computers at any other agency, and vice versa. Messages written on the C.I.A.’s network (which they still quaintly called “cables”) were purely internal. To get a message to the F.B.I. required a special communication called a “telegraphic dissemination.” Each agency had databases to amass intelligence, but because of the air gap, other agencies could not easily search them. The divisions were partly because of turf battles and partly because of legal restrictions — but they were also technological. Mike Scheuer, an adviser to the C.I.A.’s bin Laden unit until 2004, told me he had been frustrated by the inability of the systems to interpenetrate. “About 80 percent of C.I.A.-F.B.I. difficulties came from the fact that we couldn’t communicate with one another,” he said. Scheuer told me he would often send a document electronically to the F.B.I., then call to make sure the agents got it. “And they’d say, ‘We can’t find it, can you fax it?’ And then we’d call, and they’d say, ‘Well, the system said it came in, but we still can’t find it — so could you courier it over?’ ” “

These systems have served us very well for five decades,” Dale Meyerrose told me when I spoke with him recently. But now, he said, they’re getting in the way. “The 16 intelligence organizations of the U.S. are without peer. They are the best in the world. The trick is, are they collectively the best?”

Last year, Meyerrose, a retired Air Force major general, was named the chief information officer — the head computer guy, as it were — for the office of the director of national intelligence. Established by Congress in

2004, the D.N.I.'s office has a controversial mandate: it is supposed to report threats to the president and persuade the intelligence agencies to cooperate more closely. Both tasks were formerly the role of the C.I.A. director, but since the C.I.A. director had no budgetary power over the other agencies, they rarely heeded his calls to pass along their secrets. So the new elevated position of national-intelligence director was created; ever since, it has been filled by John Negroponte. Last December, Negroponte hired Meyerrose and gave him the daunting task of developing mechanisms to allow the various agencies' aging and incompatible systems to swap data. Right away, Meyerrose ordered some sweeping changes. In the past, each agency chose its own outside contractor to build customized software — creating proprietary systems, each of which stored data in totally different file formats. From now on, Meyerrose said, each agency would have to build new systems using cheaper, off-the-shelf software so they all would be compatible. But bureaucratic obstacles were just a part of the problem Meyerrose faced. He was also up against something deeper in the DNA of the intelligence services. "We've had this 'need to know' culture for years," Meyerrose said. "Well, we need to move to a 'need to share' philosophy."

There was already one digital pipeline that joined the agencies (though it had its own limitations): Intelink, which connects most offices in each intelligence agency. It was created in 1994 after C.I.A. officials saw how the Web was rapidly transforming the way private-sector companies shared information. Intelink allows any agency to publish a Web page, or put a document or a database online, secure in the knowledge that while other agents and analysts can access it, the outside world cannot.

So why hasn't Intelink given young analysts instant access to all secrets from every agency? Because each agency's databases, and the messages flowing through their internal pipelines, are not automatically put onto Intelink. Agency supervisors must actively decide what data they will publish on the network — and their levels of openness vary. Some departments have created slick, professional sites packed full of daily alerts and searchable collections of their reports going back years. Others have put up little more than a "splash page" announcing they exist. Operational information — like details of a current covert action — is rarely posted, usually because supervisors fear that a leak could jeopardize a delicate mission.

Nonetheless, Intelink has grown to the point that it contains thousands of agency sites and several hundred databases. Analysts at the various agencies generate 50,000 official reports a year, many of which are posted to the network. The volume of material online is such that analysts now face a new problem: data overload. Even if they suspect good information might exist on Intelink, it is often impossible to find it. The system is poorly indexed, and its internal search tools perform like the pre-Google search engines of the '90s."

One of my daily searches is for words like 'Afghanistan' or 'Taliban,' " I was told by one young military analyst who specializes in threats from weapons of mass destruction. (He requested anonymity because he isn't authorized to speak to reporters.) "So I'm looking for reports from field agents saying stuff like, 'I'm out here, and here's what I saw,' " he continued. "But I get to my desk and I've got, like, thousands a day — mountains of information, and no way to organize it."

Adding to the information glut, there's an increasingly large amount of data to read outside of Intelink. Intelligence analysts are finding it more important to keep up with "open source" information — nonclassified material published in full public view, like newspapers, jihadist blogs and discussion boards in

foreign countries. This adds ever more calories to the daily info diet. The W.M.D. analyst I spoke to regularly reads the blog of Juan Cole, a University of Michigan professor known for omnivorous linking to, and acerbic analysis of, news from the Middle East. “He’s not someone spies would normally pay attention to, but now he’s out there — and he’s a subject-matter expert, right?” the analyst said.

Intelligence hoarding presented one set of problems, but pouring it into a common ocean, Meyerrose realized soon after moving into his office, is not the answer either. “Intelligence is about looking for needles in haystacks, and we can’t just keep putting more hay on the stack,” he said. What the agencies needed was a way to take the thousands of disparate, unorganized pieces of intel they generate every day and somehow divine which are the most important.

Intelligence heads wanted to try to find some new answers to this problem. So the C.I.A. set up a competition, later taken over by the D.N.I., called the Galileo Awards: any employee at any intelligence agency could submit an essay describing a new idea to improve information sharing, and the best ones would win a prize. The first essay selected was by Calvin Andrus, chief technology officer of the Center for Mission Innovation at the C.I.A. In his essay, “The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community,” Andrus posed a deceptively simple question: How did the Internet become so useful in helping people find information?

Andrus argued that the real power of the Internet comes from the boom in self-publishing: everyday people surging online to impart their thoughts and views. He was particularly intrigued by Wikipedia, the “reader-authored” encyclopedia, where anyone can edit an entry or create a new one without seeking permission from Wikipedia’s owners. This open-door policy, as Andrus noted, allows Wikipedia to cover new subjects quickly. The day of the London terrorist bombings, Andrus visited Wikipedia and noticed that barely minutes after the attacks, someone had posted a page describing them. Over the next hour, other contributors — some physically in London, with access to on-the-spot details — began adding more information and correcting inaccurate news reports. “You could just sit there and hit refresh, refresh, refresh, and get a sort of ticker-tape experience,” Andrus told me. What most impressed Andrus was Wikipedia’s self-governing nature. No central editor decreed what subjects would be covered. Individuals simply wrote pages on subjects that interested them — and then like-minded readers would add new facts or fix errors. Blogs, Andrus noted, had the same effect: they leveraged the wisdom of the crowd. When a blogger finds an interesting tidbit of news, he posts a link to it, along with a bit of commentary. Then other bloggers find that link and, if they agree it’s an interesting news item, post their own links pointing to it. This produces a cascade effect. Whatever the first blogger pointed toward can quickly amass so many links pointing in its direction that it rockets to worldwide notoriety in a matter of hours.

Spies, Andrus theorized, could take advantage of these rapid, self-organizing effects. If analysts and agents were encouraged to post personal blogs and wikis on Intelink — linking to their favorite analyst reports or the news bulletins they considered important — then mob intelligence would take over. In the traditional cold-war spy bureaucracy, an analyst’s report lived or died by the whims of the hierarchy. If he was in the right place on the totem pole, his report on Soviet missiles could be pushed up higher; if a supervisor chose to ignore it, the report essentially vanished. Blogs and wikis, in contrast, work democratically. Pieces of intel would receive attention merely because other analysts found them interesting. This grass-roots process, Andrus argued, suited the modern intelligence challenge of sifting through thousands of disparate clues: if a

fact or observation struck a chord with enough analysts, it would snowball into popularity, no matter what their supervisors thought.

A profusion of spy blogs and wikis would have another, perhaps even more beneficial impact. It would drastically improve the search engines of Intelink. In a paper that won an honorable mention in the Galileo Awards, Matthew Burton — the young former D.I.A. analyst — made this case. He pointed out that the best Internet search engines, including Google, all use "link analysis" to measure the authority of documents. When you type the search "Afghanistan" into Google, it finds every page that includes that word. Then it ranks the pages in part by how many links point to the page — based on the idea that if many bloggers and sites have linked to a page, it must be more useful than others. To do its job well, Google relies on the links that millions of individuals post online every day.

This, Burton pointed out, is precisely the problem with Intelink. It has no links, no social information to help sort out which intel is significant and which isn't. When an analyst's report is posted online, it does not include links to other reports, even ones it cites. There's no easy way for agents to link to a report or post a comment about it. Searching Intelink thus resembles searching the Internet before blogs and Google came along — a lot of disconnected information, hard to sort through. If spies were encouraged to blog on Intelink, Burton reasoned, their profuse linking could mend that situation. "

Imagine having tools that could spot emerging patterns for you and guide you to documents that might be the missing pieces of evidence you're looking for," Burton wrote in his Galileo paper. "Analytical puzzles, like terror plots, are often too piecemeal for individual brains to put together. Having our documents aware of each other would be like hooking several brains up in a line, so that each one knows what the others know, making the puzzle much easier to solve."

With Andrus and Burton's vision in mind, you can almost imagine how 9/11 might have played out differently. In Phoenix, the F.B.I. agent Kenneth Williams might have blogged his memo noting that Al Qaeda members were engaging in flight-training activity. The agents observing a Qaeda planning conference in Malaysia could have mentioned the attendance of a Saudi named Khalid al-Midhar; another agent might have added that he held a multi-entry American visa. The F.B.I. agents who snared Zacarias Moussaoui in Minnesota might have written about their arrest of a flight student with violent tendencies. Other agents and analysts who were regular readers of these blogs would have found the material interesting, linked to it, pointed out connections or perhaps entered snippets of it into a wiki page discussing this new trend of young men from the Middle East enrolling in pilot training.

As those four original clues collected more links pointing toward them, they would have amassed more and more authority in the Intelink search engine. Any analysts doing searches for "Moussaoui" or "Al Qaeda" or even "flight training" would have found them. Indeed, the original agents would have been considerably more likely to learn of one another's existence and perhaps to piece together the topography of the 9/11 plot. No one was able to prevent 9/11 because nobody connected the dots. But in a system like this, as Andrus's theory goes, the dots are inexorably drawn together. "Once the intelligence community has a robust and mature wiki and blog knowledge-sharing Web space," Andrus concluded in his essay, "the nature of intelligence will change forever."

At first glance, the idea might seem slightly crazy. Outfit the C.I.A. and the F.B.I. with blogs and wikis? In the civilian world, after all, these online tools have not always amassed the most stellar reputations. There are many valuable blogs and wikis, of course, but they are vastly outnumbered by ones that exist to compile useless ephemera, celebrity gossip and flatly unverifiable assertions. Nonetheless, Andrus's ideas struck a chord with many very senior members of the office of the director of national intelligence. This fall, I met with two of them: Thomas Fingar, the patrician head of analysis for the D.N.I., and Mike Wertheimer, his chief technology officer, whose badge clip sports a button that reads "geek." If it is Meyerrose's job to coax spy hardware to cooperate, it is Fingar's job to do the same for analysts.

Fingar and Wertheimer are now testing whether a wiki could indeed help analysts do their job. In the fall of 2005, they joined forces with C.I.A. wiki experts to build a prototype of something called Intellipedia, a wiki that any intelligence employee with classified clearance could read and contribute to. To kick-start the content, C.I.A. analysts seeded it with hundreds of articles from nonclassified documents like the C.I.A. World Fact Book. In April, they sent out e-mail to other analysts inviting them to contribute, and sat back to see what happened.

By this fall, more than 3,600 members of the intelligence services had contributed a total of 28,000 pages. Chris Rasmussen, a 31-year-old "knowledge management" engineer at the National Geospatial-Intelligence Agency, spends part of every day writing or editing pages. Rasmussen is part of the younger generation in the intelligence establishment that is completely comfortable online; he regularly logs into a sprawling, 50-person chat room with other Intellipedians, and he also blogs about his daily work for all other spies to read. He told me the usefulness of Intellipedia proved itself just a couple of months ago, when a small two-seater plane crashed into a Manhattan building. An analyst created a page within 20 minutes, and over the next two hours it was edited 80 times by employees of nine different spy agencies, as news trickled out. Together, they rapidly concluded the crash was not a terrorist act. "In the intelligence community, there are so many 'Stay off the grass' signs," Rasmussen said. "But here, you're free to do what you want, and it works."

By the late summer, Fingar decided the Intellipedia experiment was sufficiently successful that he would embark on an even more high-profile project: using Intellipedia to produce a "national intelligence estimate" for Nigeria. An N.I.E. is an authoritative snapshot of what the intelligence community thinks about a particular state — and a guide for foreign and military policy. Nigeria, Fingar said, is a complex country, with issues ranging from energy to Islamic radicalism to polio outbreaks to a coming election. Intellipedia's Nigeria page will harness the smarts of the dozen or so analysts who specialize in the country. But it will also, Fingar hopes, attract contributions from other intelligence employees who have expertise Fingar isn't yet aware of — an analyst who served in the Peace Corps in Nigeria, or a staff member who has recently traveled there. In the traditional method of producing an intelligence estimate, Fingar said, he would call every agency and ask to borrow their Africa expert for a week or two of meetings. "And they'd say: 'Well, I only got one guy who can spell Nigeria, and he's traveling. So you lose.' " In contrast, a wiki will "change the rules of who can play," Fingar said, since far-flung analysts and agents around the world could contribute, day or night.

Yet Intellipedia also courts the many dangers of wikis — including the possibility of error. What's to stop analysts from posting assertions that turn out to be false? Fingar admits this will undoubtedly happen. But

if there are enough people looking at an entry, he says, there will always be someone to catch any grave mistakes. Rasmussen notes that though there is often strong disagreement and debate on Intellipedia, it has not yet succumbed to the sort of vandalism that often plagues Wikipedia pages, including the posting of outright lies. This is partly because, unlike with Wikipedia, Intellipedia contributors are not anonymous. Whatever an analyst writes on Intellipedia can be traced to him. “If you demonstrate you’ve got something to contribute, hey, the expectation is you’re a valued member,” Fingar said. “You demonstrate you’re an idiot, that becomes known, too.”

While the C.I.A. and Fingar’s office set up their wiki, Meyerrose’s office was dabbling in the other half of Andrus’s equation. In July, his staff decided to create a test blog to collect intelligence. It would focus on spotting and predicting possible avian-flu outbreaks and function as part of a larger portal on the subject to collect information from hundreds of sources around the world, inside and outside of the intelligence agencies. Avian flu, Meyerrose reasoned, is a national-security problem uniquely suited to an online-community effort, because information about the danger is found all over the world. An agent in Southeast Asia might be the first to hear news of dangerous farming practices; a medical expert in Chicago could write a crucial paper on transmission that was never noticed by analysts.

In August, one of Meyerrose’s assistants sat me down to show me a very brief glimpse of the results. In the months that it has been operational, the portal has amassed 38,000 “active” participants, though not everyone posts information. In one corner was the active-discussion area — the group blog where the participants could post their latest thoughts about avian flu and others could reply and debate. I noticed a posting, written by a university academic, on whether the H5N1 virus could actually be transmitted to humans, which had provoked a dozen comments. “See, these people would never have been talking before, and we certainly wouldn’t have heard about it if they did,” the assistant said. By September, the site had become so loaded with information and discussion that Rear Adm. Arthur Lawrence, a top official in the health department, told Meyerrose it had become the government’s most crucial resource on avian flu.

The blog seemed like an awfully modest thing to me. But Meyerrose insists that the future of spying will be revolutionized as much by these small-bore projects as by billion-dollar high-tech systems. Indeed, he says that overly ambitious projects often result in expensive disasters, the way the F.B.I.’s $170 million attempt to overhaul its case-handling software died in 2005 after the software became so complex that the F.B.I. despaired of ever fixing the bugs and shelved it. In contrast, the blog software took only a day or two to get running. “We need to think big, start small and scale fast,” Meyerrose said.

Moving quickly, in fact, is crucial to building up the sort of critical mass necessary to make blogs and wikis succeed. Back in 2003, a Department of Defense agency decided to train its analysts in the use of blog software, in hopes that they would begin posting about their work, read one another’s blogs and engage in productive conversations. But the agency’s officials trained only small groups of perhaps five analysts a month. After they finished their training, those analysts would go online, excited, and start their blogs. But they’d quickly realize no one else was reading their posts aside from the four other people they’d gone through the training with. They’d get bored and quit blogging, just as the next trainees came online.

There was never a tipping point — “never a moment when two people who never knew each other could begin discussing something,” as Clay Shirky, a professor at New York University who was hired to consult

on the project, explained to me. For the intelligence agencies to benefit from "social software," he said, they need to persuade thousands of employees to begin blogging and creating wikis all at once. And that requires a cultural sea change: persuading analysts, who for years have survived by holding their cards tightly to their chests, to begin openly showing their hands online.

Is it possible to reconcile the needs of secrecy with such a radically open model for sharing? Certainly, there would be merit in a system that lets analysts quickly locate like-minded colleagues around the world to brainstorm new ideas about how the Iraqi insurgency will evolve. But the intelligence agencies also engage in covert operations that ferret out truly incendiary secrets: the locations of Iranian nuclear facilities, say, or the name of a Qaeda leader in Pakistan. Is this the sort of information that is safe to share widely in an online network?

Many in the intelligence agencies suspect not. Indeed, they often refuse to input sensitive intel into their own private, secure databases; they do not trust even their own colleagues, inside their own agencies, to keep their secrets safe. When the F.B.I. unveiled an automated case-support system in 1995, agents were supposed to begin entering all information from their continuing cases into it, so that other F.B.I. agents could benefit from the collected pool of tips. But many agents didn't. They worried that a hard-won source might be accidentally exposed by an F.B.I. agent halfway across the country. Worse, what would happen if a hacker or criminal found access to the system?

These are legitimate concerns. After the F.B.I. agent Robert Hanssen was arrested for selling the identities of undercover agents to Russia, it turned out he had found their names by trawling through records on the case-support system. As a result, many F.B.I. agents opted to keep their records on paper instead of trusting the database — even, occasionally, storing files in shoeboxes shoved under their desks. "When you have a source, you go to extraordinary lengths to protect their identities," I. C. Smith, a 25-year veteran of the bureau, told me. "So agents never trusted the system, and rightly so."

Worse, data errors that allow information to leak can often go undetected. Five years ago, Zalmai Azmi — currently the chief information officer of the F.B.I. — was working at the Department of Justice on a data-sharing project with an intelligence agency. He requested data that the agency was supposed to have scrubbed clean of all classified info. Yet when it arrived, it contained secret information. What had gone wrong? The agency had passed it through filters that removed any document marked "secret" — but many documents were stamped "SECRET," in uppercase, and the filter didn't catch the difference. The next time Azmi requested documents, he found yet more secret documents inadvertently leaked. This time it was because the documents had "S E C R E T" typed with a space between each letter, and the filter wasn't programmed to catch that either.

A spy blogosphere, even carefully secured against intruders, might be fundamentally incompatible with the goal of keeping secrets. And the converse is also true: blogs and wikis are unlikely to thrive in an environment where people are guarded about sharing information. Social software doesn't work if people aren't social.

Virtually all proponents of improved spy sharing are aware of this friction, and they have few answers. Meyerrose has already strained at boundaries that make other spies deeply uneasy. During the summer, he

set up a completely open chat board on the Internet and invited anyone interested to participate in a two-week-long discussion of how to improve the spy agencies' policies for acquiring new technology.

The chat room was unencrypted and unsecured, so anyone could drop in and read the postings or mouth off. That way, Meyerrose figured, he'd be more likely to get drop-ins by engineers from small, scrappy start-up software firms who might have brilliant ideas but no other way to get an audience with intelligence chiefs. The chat room provoked howls of outrage. "People were like, 'Hold it, can't the Chinese and North Koreans listen in?' " Meyerrose told me. "And, sure, they could. But we weren't going to be discussing state secrets. And the benefits of openness outweigh the risks."

For something like Intellipedia, though, which trafficks in genuinely serious intelligence, hard decisions had to be made about what risks were acceptable. Fingar says that deeply sensitive intel would never be allowed onto Intellipedia — particularly if it was operational information about a mission, like a planned raid on a terrorist compound. Indeed, Meyerrose's office is building three completely separate versions of Intellipedia for each of the three levels of secrecy: Top Secret, Secret and Unclassified. Each will be placed on a data network configured so that only people with the correct level of clearance can see them — and these networks are tightly controlled, so sensitive information typed into the Top Secret Intellipedia cannot accidentally leak into the Unclassified one.

But will this make the Intellipedia less useful? There are a few million government employees who could look at the relatively unsecret Intellipedia. In contrast, only a few thousand intelligence officials qualify for a Top Secret clearance, and thus will be allowed into the elite version. This presents a secrecy paradox. The Unclassified Intellipedia will have the biggest readership and thus will grow the most rapidly; but if it's devoid of truly sensitive secrets, will it be of any use?

Fingar says yes, for an interesting reason: top-secret information is becoming less useful than it used to be. "The intelligence business was initially, if not inherently, about secrets — running risks and expending a lot of money to acquire secrets," he said, with the idea that "if you limit how many people see it, it will be more secure, and you will be able to get more of it. But that's now appropriate for a small and shrinking percentage of information." The time is past for analysts to act like "monastic scholars in a cave someplace," he added, laboring for weeks or months in isolation to produce a report.

Fingar says that more value can be generated by analysts sharing bits of "open source" information — the nonclassified material in the broad world, like foreign newspapers, newsletters and blogs. It used to be that on-the-ground spies were the only ones who knew what was going on in a foreign country. But now the average citizen sitting in her living room can peer into the debates, news and lives of people in Iran. "If you want to know what the terrorists' long-term plans are, the best thing is to read their propaganda — the stuff out there on the Internet," the W.M.D. analyst told me. "I mean, it's not secret. They're telling us."

Fingar and Andrus and other intelligence thinkers do not play down the importance of covert ops or high-tech satellite surveillance in intercepting specific jihadist plots. But in a world that is awash in information, it is possible, they say, that the meaning of intelligence is shifting. Beat cops in Indiana might be as likely to uncover evidence of a terror plot as undercover C.I.A. agents in Pakistan. Fiery sermons printed on pamphlets in the U.K. might be the most valuable tool in figuring out who's raising money for a

possible future London bombing. The most valuable spy system is one that can quickly assemble disparate pieces that are already lying around — information gathered by doctors, aid workers, police officers or security guards at corporations.

The premise of spy-blogging is that a million connected amateurs will always be smarter than a few experts collected in an elite star chamber; that Wikipedia will always move more quickly than the Encyclopaedia Britannica; that the country's thousand-odd political bloggers will always spot news trends more quickly than slow-moving journalists in the mainstream media. Yet one of the most successful new terrorism-busting spy organizations since 9/11 does in fact function like a star chamber. The National Counterterrorism Center was established by Congress in 2004 and charged with spotting the most important terrorism threats as they emerge. The counterterrorism center is made up of representatives from every intelligence agency — C.I.A., F.B.I., N.S.A. and others — who work together under one roof. Each analyst has access to details particular to his or her agency, and they simply share information face to face. The analysts check their personal networks for the most dire daily threats and bring them to the group. In three meetings a day, the officials assess all the intel that has risen to their attention — and they jointly decide what the nation's most serious threats are. "We call it carbon-based integration," said William Spalding, the center's chief information officer.

When I raised the idea of collaborative tools like blogs and wikis, Spalding and Russ Travers, one of the center's deputy directors, were skeptical. The whole reason the center works, they said, is that experts have a top-down view that is essential to picking the important information out of the surrounding chatter. The grass roots, they've found, are good at collecting threats but not necessarily at analyzing them. If a lot of low-level analysts are pointing to the same inaccurate posting, that doesn't make it any less wrong."

The key is to have very smart people culling" the daily tips, Travers told me. In October, for example, nervous rumors that a football stadium in the United States would be subject to a nuclear attack flooded the National Counterterrorism Center; analysts there immediately suspected it was spurious. "The terrorist problem has the worst signal-to-noise ratio," Travers said. Without the knowledge that comes from long experience, he added, a fledgling analyst or spy cannot know what is important or not. The counterterrorism center, he said, should decide which threats warrant attention. "That's our job," he said.

The Spying 2.0 vision has thus created a curious culture battle in intelligence circles. Many of the officials at the very top, like Fingar, Meyerrose and their colleagues at the office of the director of national intelligence, are intrigued by the potential of a freewheeling, smart-mobbing intelligence community. The newest, youngest analysts are in favor of it, too. The resistance comes from the "iron majors" — career officers who occupy the enormous middle bureaucracy of the spy agencies. They might find the idea of an empowered grass roots to be foolhardy; they might also worry that it threatens their turf.

And the critics might turn out to be right. As Clay Shirky of N.Y.U. points out, most wikis and blogs flop. A wiki might never reach a critical mass of contributors and remain anemic until eventually everyone drifts away; many bloggers never attract any attention and, discouraged, eventually stop posting. Wikipedia passed the critical-mass plateau a year ago, but it is a rarity. "The normal case for social software is failure," Shirky said. And because Intellipedia is now a high-profile experiment with many skeptics, its failure could permanently doom these sorts of collaborative spy endeavors.

There is also the practical question of running a huge civil-service agency where you have to assess the performance of your staff. It might be difficult to measure contributions to a wiki; if a brilliant piece of analysis emerges from the mob, who gets credit for it? “A C.I.A. officer’s career is advanced by producing reports,” notes David Weinberger, a fellow at the Harvard Berkman Center for the Internet and Society, who consulted briefly with the C.I.A. on its social software. “His ability is judged by those reports. And that gets in the way of developing knowledge socially, where it becomes very difficult to know who added or revised what.”

In addition, civil libertarians are alarmed by the idea of spies casually passing sensitive information around from one agency to another. “I don’t want the N.S.A. passing on information about innocent Americans to local cops in San Diego,” Weinberger said. “Those laws exist for good reasons.”

In many ways, the new generation of Web-savvy spies frames the same troubling questions as the Patriot Act, which sought to break down the barriers preventing military spy agencies from conducting operations inside the United States, on American citizens, and then sharing that information with domestic groups. On a sheerly practical level, it makes sense to get rid of all barriers: why not let the N.S.A. wiretap American conversations? Vice President Cheney has argued forcefully that these historical barriers between agencies hobble the American military and intelligence forces; the Patriot Act was designed in part to eliminate them. Terrorist groups like Al Qaeda heed no such boundaries, which is precisely why they can move so quickly and nimbly.

Then again, there’s a limit to how much the United States ought to emulate Al Qaeda’s modus operandi. “The problems the spies face are serious; I sympathize with that,” Shirky told me. “But they shouldn’t be wiping up every bit of information about every American citizen.” The Pentagon’s infamous Total Information Awareness program, which came to light in 2002, was intended to scoop up information on citizens from a variety of sources — commercial purchase databases, government records — and mine it for suggestive terrorism connections. But to many Americans, this sort of dot-connecting activity seemed like an outrageous violation of privacy, and soon after it was exposed, the program was killed. James X. Dempsey, director of the Center for Democracy and Technology, maintains that the laws on spying and privacy need new clarity. The historic morass of legislation, including the Patriot Act, has become too confusing, he says; both spies and the public are unsure what walls exist. While Dempsey agrees that agencies should probably be allowed to swap more information than they currently do, he says that revamped rules must also respect privacy — “otherwise, we’ll keep on producing programs that violate people’s sense of what’s right, and they’ll keep getting shut down.”

For all the complaints about hardware, the challenges are only in part about technology. They are also about political will and institutional culture — and whether the spy agencies can be persuaded to change. Some former intelligence officials have expressed skepticism about whether Meyerrose and Fingar and their national-intelligence colleagues have the clout and power to persuade the agencies to adopt this new paradigm. Though D.N.I. officials say they have direct procurement authority over technology for all the agencies, there’s no evidence yet that Meyerrose will be able to make a serious impact on the eight spy agencies in the Department of Defense, which has its own annual $38 billion intelligence budget — the lion’s share of all the money the government spends on spying. When I spoke to Wilson P. Dizard III, a writer with Government Computer News who has covered federal technology issues for two decades, he

said, “You have all these little barons at N.S.A. and C.I.A. and whatever, and a lot of people think they’re not going to do what the D.N.I. says, if push comes to shove.”

Today’s spies exist in an age of constant information exchange, in which everyday citizens swap news, dial up satellite pictures of their houses and collaborate on distant Web sites with strangers. As John Arquilla told me, if the spies do not join the rest of the world, they risk growing to resemble the rigid, unchanging bureaucracy that they once confronted during the cold war. “Fifteen years ago we were fighting the Soviet Union,” he said. “Who knew it would be replicated today in the intelligence community?”

Clive Thompson, a contributing writer, last wrote for the magazine about Google’s business dealings in China.

Cyber spying, or cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers, cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online Open Source Spy is another one of those binary option software programs that come out every day. Its not the first and it won't be the last. Whom ever is behind Open Source Spy presented by Jake Miller is not important because the man presenting in the video is most likely an actor. This Happens all the time. There is no indication he is even one of them. I've traced actors from IMDB on these type on products myself. Please check to see if Open Source Spy are using a regulated broker if you chose to use this program. Awesome Open Source. Sponsorship. Combined Topics.Â A Stealthy Trojan Spyware (keylogger-spyware-malware-worm-spy-virus-fud-undetectable-computer-windows-pc-c-c++). Adobot â335. Open-source android spyware. Stupidkeylogger â292. A Terrific Keystroke Recorder (keylogger-key-logger-spyware-spy-trojan-simple-virus-for-windows-10-7-xp-smart-c-c++-cpp-code). Richkware â285. Framework for building Windows malware, written in C++.