The Electronic Donut Shop: Networking in the Information Age[1]

by
Bernard H. Levin[2]
Carl J. Jensen III[3]

Late in 2004, one of the authors attended a conference session with many of the Amovers and shakers@ in the law enforcement intelligence world. When someone asked the audience whether it was easier to get information through official "sharing" channels or just to call a friend, there was unanimity that calling a friend was still the way to go.

In spite of boundless good intentions, hard work, and the involvement of many bright, capable folks, intelligence sharing remains piecemeal, to put it charitably. However there was a clue: in science, when the prevailing paradigm refuses to yield satisfactory results, perhaps it=s time to change paradigms. That is precisely what we suggest in the next few pages.

We contend that the donut shop of your past (and the present) has gotten a bad rap. Yes, it was not always great for our professional image nor for our diet, but it had one virtue often overlooked by police managers and virtually unknown to the general public. The donut shop provided a venue for peer-to-peer information sharing. It is this sharing function that led to our choice of the donut shop metaphor.

It=s About the Network

In one sense, the police are exactly suited for the information age: every officer or agent understands networks. Back in the days of buggy whips and MS-DOS, cops swapped information while drinking coffee in a donut shop. Those sharing sessions got around hierarchy, but didn't have much breadth. For an officer in a small agency, finding someone at LAPD or NYPD could be accomplished, but it wasn't easy. Then came the widespread use of the Internet. For the past decade, we have had electronic donut shops where we literally can talk as easily with a cop on the other side of the world as with a cop on the adjacent beat. And we do. Lots of tactical and strategic information gets passed that way, even though the hierarchy typically hasn't a clue.

The organization of traditional intelligence and its highly correlated security classification system are vestiges of the industrial age. In the information age, data and information have decreasing shelf life, so speed is valued. Speed and hierarchy are incompatible. What does the electronic donut shop concept offer? It mercilessly increases speed by flattening hierarchy and provides power to those at all levels in the chain, under the assumption that EVERYONE, from the beat cop in the 3-person agency to the federal intelligence analyst, has a role to play.

The Concept

A plethora of studies from the social sciences and elsewhere suggest that the most efficient way to create a system that folks will embrace is from the bottom up. Why should intelligence be any different? People in the federal government and in many large local police departments have been working feverishly since 9-11 to create better intelligence systems and there is good reason to believe that progress has been made. Yet, few local police agencies have changed the way they do business in any meaningful way. Nor have the essentially hierarchical relationships among local, state, federal and tribal entities changed much. Where the few useful changes have taken place, they have been more informal, line-to-line rather than agency-to-agency. How can we correct this?

Chaos theory informs us that high levels of order emerge from activity that may appear random and chaotic. Upon reviewing an early draft of this article, one of our colleagues noted:

> When people try to establish systems controlling the interactions and relationships between other people do they not automatically create hierarchies? The beauty of the Internet and related IT systems is that they are not a human system, they're a technological system that facilitates human communication. The underlying premise that we have been working from trying to solve this information sharing problem is that we are capable of engineering or establishing some kind of efficient human system between people that will make them share information. We believe that if we simply decree that there will be more cooperation, fewer silos, and less bureaucracy, and people actually do it, that solves the problem. But is that the way it works? Maybe the premise should be that human networks are created when we give them the tools to communicate freely.[4]

One point resonated clearly with us: A system that comes together as a result of the efforts of those who eventually have to use it works better than one imposed from somewhere else. All of us have worked on task forces; our experience has been that task forces that form from the ground up (that is, as the result of front line troops organizing themselves) work better than those organized by the high command. To that end, regionalized task forces, organized at the local level and made up of local, state, federal, tribal or other entities (e.g., military, private sector) will be less a luxury than an essential function as we navigate the 21st century.

But that, really, is only the first step. Imagine the construction of a virtual rather than physical task force with EVERYONE engaged in the intel business. Imagine operators freely and openly sharing information and ideas with one another. The electronic donut shop.

Technology Can Help

It has been estimated that by 2010, the body of known information will double every 75 days.
Dr. Evan T. Robinson[5]

Even today, we are awash in information. Who among us has enough time to read all we should? The challenge of the information age is not the lack of information B rather, we need to figure out how to manage and effectively use what we have. To some degree, that has already happened outside of policing: Data mining is being used extensively in the private sector with some extraordinary success. Policing needs to get onboard or risk irrelevance.

A small example from another of our colleagues:

> Informal conversations can be electronically analyzed. This is nothing new in computer science. There are many examples of applications that extract meaning and intent from conversations, in particular in psychology. Imagine two intel analysts chatting with each other while a 'bot[6] analyzes their conversation in real time. Not only is the information they exchange stored somewhere for future analysis (if the analysts so desire), but the content of their conversation is examined for intent. Based on what the 'bot finds, it then goes out to its knowledge base and looks for any other information that might be of use to the analysts. For example, if two people are talking about an incident involving stolen fertilizer, it might come back and say "hey, look what I found in Nebraska and Oklahoma! Two similar cases. Here are the people you want to talk to. Here is a map showing the incidents. Here is a link chart of all the people involved. And, finally, here is a timeline of when these incidents occurred relative to your two incidents. Oh, and would you like me to contact the intel analysts involved in those cases and bring them in on the conversation?"[7]

Yeah, But....

By now, those still reading may harbor many reservations. We will attempt to address two here.

Privacy: Those who follow the news no doubt recall the blistering attacks leveled against intelligence initiatives such as the Total Information Awareness & MATRIX programs.[8] Civil liberties and privacy concerns should never be casually or trivially dismissed. Nevertheless, the authors agree with noted attorney Alan Dershowitz who draws a distinction between Aprivacy@ and Aanonymity:@

> (T)here is the question of the right to anonymity. I don't believe we can afford to recognize such a right in this age of terrorism. No such right is hinted at in the Constitution. And though the Supreme Court has identified a right to privacy, privacy and anonymity are not the same. American taxpayers, voters and drivers long ago gave up any right of anonymity without loss of our right to engage in lawful conduct within zones of privacy. Rights are a function of experience, and our recent experiences teach that it is far too easy to be anonymous C even to create a false identity C in this large and decentralized country.[9]

Information Security: There are many reasons that information is not shared; one of the main ones is reflected in Franklin=s admonition that Athree may keep a secret, if two of them are dead.@[10] In today=s environment of chronic leakage, one is tempted to believe him. Yet, the problem may be one of conceptualization more than anything else. If we treated the information under our control as we treat the firearms issued to us, many of our problems might disappear. While the comparison may seem contrived or even absurd, it is not.

We wield our weapons to save lives; we wield information similarly. When we treat our firearms carelessly, negligently, or maliciously, grave damage can result. So, too, with

information.[11] Imagine if we treated the mismanagement of information in the same serious manner that we treat the mismanagement of firearms, with meaningful investigation and, where warranted, punishment. Imagine if we afforded information training at the same level that we offer firearms training. Does anyone doubt that we would see fewer leaks or careless chatter and better information proficiency?

The carrot and the stick are not obsolete: if one shows a disregard for the prudent management of information, it can be denied to him/her. Correspondingly, if one shows that he/she can be trusted, new levels of information may be made available. And all of this can happen with virtual rather than human oversight.

What=s a Chief to Do?

Four quick recommendations:

1) Encourage those who work for you to join an electronic mailing list (EML).[12] Join one yourself. EMLs are Internet-based e-mail lists in which a message from any subscriber may be broadcast automatically to everyone else on the list. The result is not unlike that of a news group, with the exception that only individuals on the list are privy to each message. EMLs generally form around a particular group or area of interest. In the policing world, some have been around for a long time. For example, both authors are members of Police-L (http://www.police-l.org/) which describes itself as: Aa restricted list, open only to sworn law enforcement officers (LEOs), including retired, reserve and auxiliary officers. Its purpose is to serve as a forum in which LEOs can exchange information regarding local practices and procedures, discuss issues of concern or interest to them, or otherwise be free to communicate amongst themselves in a police-only setting.@[13]

Messages to Police-L can be digested, which means the recipient can opt to receive one single consolidated message per day. In addition, its restricted nature permits a free and often very candid exchange of information between members from all levels of the LEO food chain. Topics vary widely, from strongly fought political exchanges to information regarding the latest innovation in police hardware. Of perhaps greatest interest, any member with a question or quandary can submit it to the list and be confident that brother and sister officers from across the planet will weigh in with an answer or opinion.

2) Start an EML or its equivalent yourself. More and more agencies have elected to follow this course. For example, geographically-based lists for chiefs and homicide investigators have been established to share information. The FBI offers its secure Law Enforcement Online service free-of-charge (http://www.fbi.gov/hq/cjisd/leo.htm). Among its features are news and special interest groups, the latter of which can be configured to meet very specific needs.

3) Establish a relationship with a local college or university.[14] Institutions of higher learning generally have computer systems far superior to those in police agencies. As well, researchers there are often at the cutting-edge of such things as GIS, data mining, and analytical techniques. One reason more researchers aren=t working with police agencies is that they haven=t been asked. For guidance in this area, see the recent International Association of Chiefs of Police

publication entitled AImproving Partnerships Between Law Enforcement Leaders And University Based Researchers.@[15]

4) Regularly read a publication of substance that has nothing to do with policing. Given the average police executive=s busy schedule, this may seem a luxury that one can ill afford. Consider, however, the manner and rapidity at which the world around us, the world that we must police, is changing. Consider as well that our planet=s geopolitical boundaries are rapidly melting away, changing forever our definition of Ajurisdiction.@ In order to lead police to this new world, we must first have a clear sense of how it is changing around us. One way to do that is to access one (or more) of the many excellent periodicals that currently appear online. And the really good news: one can subscribe to many of these at no charge.

Conclusion

The law of least effort is among the most powerful of laws, only marginally less powerful than the law of gravity. It always will be easier to talk with friends and acquaintances than it will be to wade through hierarchy. Thus, law enforcement leaders would be wise to exploit this fact rather than to try to suppress it by means of hierarchical restrictions on users. The current age provides policing with myriad opportunities to exploit technologies and capabilities that are routine elsewhere. While neither of us is confident enough to wager a paycheck, we remain cautiously optimistic.

---

[1]The authors wish to thank their colleagues in the Futures Working Group who provided many useful and insightful comments with regard to this article. In particular, Thomas Cowper, Sandy Boyd, Andreas Olligschlaeger, and Michael Buerger were most helpful.

[2]Dr. Levin is a professor at Blue Ridge Community College; a reserve major in the Waynesboro, Virginia, Police Department; and the Vice-Chairman of the Futures Working Group.

[3]Dr. Jensen is a Special Agent assigned to the FBI=s Behavioral Science Unit. He is the Chairman of the Futures Working Group.

[4]Cowper, Thomas (2004). Personal communication with the authors.

[5]Robinson, Evan T. (Undated) ALifetime learning: Is the Internet the solution?@ at URL http://www.uspharmacist.com/oldformat.asp?url=newlook/files/Phar/lifetime_learning1.htm&pub_id=8&article_id=752 accessed 1/7/2005.

[6]Robot.

[7]Olligschlaeger, Andreas (2004) Personal communication with the authors.

[8]See, for example, http://www.aclu.org/Privacy/Privacy.cfm?ID=14240&c=130.

[9]Dershowitz, Alan (2001). AWhy fear national ID cards?@ New York Times at URL

http://www.johnlaxmi.com/WWHow/ID.htm accessed 11/21/2004.

[10]Franklin, Benjamin (undated). AThe quotable Franklin@ at URL http://www.ushistory.org/franklin/quotable/quote08.htm accessed 1/7/2005

[11]Consider, inter alia, espionage, compromised investigations, and irreparably damaged reputations.

[12]Sometimes mistakenly referred to as a ALISTSERV,@ which is the proper name of a commercially licensed product. Many law enforcement related EMLs currently exist.

[13]Police-L (undated) at URL http://www.police-l.org/about.html accessed 12/28/2004.

[14]This includes smaller colleges, including community colleges, where it may be easier to initiate and maintain mutually beneficial relationships.

[15]http://www.theiacp.org/documents/pdfs/Publications/LawEnforcement%2DUniversityPartnership%2Epdf