Integrating Virtual Public-Private Partnerships into Local Law Enforcement for Enhanced Intelligence-Led Policing

Matthew J. Simeone, Jr.

INTRODUCTION

In recent years, police chiefs and sheriffs across the nation have come to the realization that local law enforcement is on America's front lines in the effort to keep our hometowns safe from terrorism. As a result, homeland security has become an important part of every patrol officer's responsibilities.

In assuming this responsibility, many local law enforcement agencies have spent millions of dollars on specialized equipment and training exercises in order to enhance their capacity to respond to a terrorist attack. In addition, intelligence reports warning of possible terrorist attacks have prompted many agencies to sporadically ramp-up police presence at high-risk locations in an effort to prevent a terrorist act. These locations typically include transportation facilities, critical infrastructure sites, and other high profile venues. The overtime bill for some agencies has been significant.

In all, billions of dollars have been spent on equipment and personnel-related costs, much of which has been subsidized by the federal government in the attempt to provide homeland security.[1] Whether our nation can continue on this course and sustain such homeland security expenditures going forward is questionable. America's economic viability, it seems, may hinge upon the ability to develop an alternative homeland security strategy to deal with terrorism and its associated threat.

Meanwhile, the capacity for law enforcement alone to prevent crime and provide homeland security may be more limited than police generally acknowledge.[2] With an average of only one sworn officer policing every 400 residents nationwide, law enforcement must rely on the private sector to help prevent and solve crimes.[3] In addition, when considering that criminals and potential terrorists may also be living or conducting preoperational planning for terrorist acts in our communities, it becomes evident that the private sector represents the largest potential source of information for solving crime, apprehending criminals, and possibly preventing terrorist attacks. One example of a private sector contribution to public safety comes from the popular television show *America's Most Wanted*, which has helped to apprehend fugitives who have evaded arrest for years. In some cases, arrests of fugitives have come in just a matter of hours after they have been profiled on the show.

Moreover, with roughly two million people employed in private security and approximately 800,000 sworn law enforcement officers in the United States, private security makes up nearly three-quarters of the protective workforce.[4] As the vast majority of our nation's critical infrastructure is under private control, private security firms are perhaps in the best position to be "first preventers" of crime and terrorism.

Consequently, our nation's *long-term* success in preventing crime and maintaining homeland security may very well depend upon the extent to which law enforcement agencies engage in partnerships with the private sector to support their public safety mission. This paper will examine virtual public-private partnerships (VP3s) and how local law enforcement agencies can use them to enhance intelligence-led policing and,

consequently, make for safer communities. A VP3 can offer extraordinary leverage in utilizing the private sector as a force multiplier and has the potential to take policing to significantly higher levels of effectiveness.

INTERNET TECHNOLOGY

During the last decade, technology has changed the way we shop, bank, and spend our leisure time. With nearly 70 percent of American adults using the internet, telecommunications technology has revolutionized the way we communicate and has made the universe of ideas accessible to anyone with a computer and internet access.[5] It is safe to say that the private sector, with its profit-driven motivation, has exploited technology to its full advantage.

Today, we are fighting an enemy that, in many cases, is very well-networked. As law enforcement agencies turn to the business of developing their intelligence capacity, they are faced with the challenge of not only networking with other law enforcement and government agencies, but with the residential and business communities they serve as well. In most agencies, extending the law enforcement network broadly into these communities is an issue for which personnel resources are the limiting factor. In other words, an agency employs a limited number of officers who work a set number of hours per day in which they can build relationships and develop contacts within the community.

Local police and sheriffs departments, however, can now utilize internet technology to exponentially expand their law enforcement intelligence network. The term *law enforcement intelligence network* is used in this paper to describe the network of individuals to which a law enforcement agency can directly disseminate information or intelligence and from which information can be collected for use in the process of developing intelligence. Later in this paper four types of internet technologies will be discussed in the context of their use by local law enforcement. First, however, this paper will examine intelligence-led policing (ILP), a policing paradigm which is well-positioned to be on the nation's law enforcement agenda for the foreseeable future.

INTELLIGENCE-LED POLICING

After 9/11, insights into the importance of timely and actionable intelligence in preventing terrorist attacks have supported the adoption of intelligence-led policing (ILP). This method of policing, which originated over a decade ago in the United Kingdom, relies on a robust system of data collection from a wide range of sources to produce the best possible intelligence products.

One way to study what it means for policing to be "intelligence-led" is to examine the 3i Model (see Figure 1), which was introduced by Dr. Jerry Ratcliffe.[6] This model represents a method of crime reduction utilizing an intelligence-led process. It also provides an overarching framework for understanding ILP.

The 3i Model consists of three essential structures: an intelligence structure or unit, the criminal environment, and the decision maker. In addition, there are three processes which represent the 3 "i"s. They are: to interpret, influence, and impact (see Figure 1).

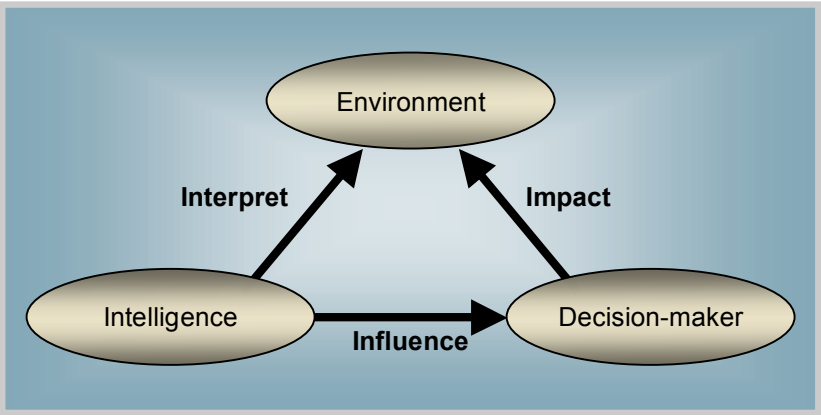

Figure 1. Ratcliffe's 3i Model of Intelligence-Led Policing

Adapted from J. H. Ratcliffe, "Intelligence-Led Policing." *Trends and Issues in Crime and Criminal Justice* No. 248 (2003): 3.

The first stage of the model involves the interpretation of the criminal environment by the intelligence structure. Recognizing that this environment is fluid, the intelligence structure collects data from both within and external to the agency in an attempt to paint as complete a picture as possible in creating its intelligence product. This will assist the second stage, which involves identifying decision makers and then developing intelligence products that can influence them. The third stage relies on the decision makers having the creativity and skills to positively impact the criminal environment and reduce crime.

In describing the 3i Model as a crime reduction process, Ratcliffe notes the importance of local partnerships and acknowledges that decision makers may also exist outside of police agencies. A comprehensive intelligence system, he says, can recognize this and influence a broad range of internal and external decision makers.[7] This speaks to the need for the intelligence unit within an agency to be able to produce intelligence products for a wide variety of consumers.

In looking at the relationship between virtual public-private partnerships and intelligence-led policing, we find that a VP3 can better enable agencies to connect with the communities they serve, exponentially expand their law enforcement intelligence network into the private sector, and, in turn, create much greater capacity for both information collection and dissemination. In addition, the greater the range of data sources and the more robust the intelligence network, the greater the chance that analysts will be able to paint an accurate intelligence picture. This can facilitate better intelligence products, which better enables decision-makers to impact the criminal environment.

This paper will study how local law enforcement agencies can integrate virtual public-private partnerships and enhance intelligent-led policing in a way that will result in: 1) a more informed and engaged private sector that can assist in preventing crime and terrorism; 2) more relevant and valuable information flowing from the private sector into the intelligence cycle; and 3) better intelligence which can drive better decision making.

"ALL-CRIMES, ALL-THREATS, ALL-HAZARDS"

In developing a VP3, an agency will need to decide on the scope of the partnership. The NYPD, in forming Shield, chose a clear counterterrorism focus.[8] Elsewhere in the New York metropolitan area, the Nassau County Police Department's Security/Police Information Network (SPIN) and the Suffolk County Police Department's Suffolk County Alert Network (SCAN) have both taken an "all-crimes, all-threats, all-hazards" approach.[9] Although the needs of jurisdictions may vary (and while the threat of terrorism may be greater in one jurisdiction and the threat of natural disaster greater in another) to some extent law enforcement agencies everywhere must deal with all three of these domains. Once the resources to administer a partnership are in place, taking a broad "all-crimes, all-threats, all-hazards" approach gives the law enforcement agency the greatest return on investment and offers the most value and utility to both users and the agency involved.

For users, an "all-crimes, all-threats, all-hazards" VP3 becomes a place for one-stop shopping for a variety of information needs. From counterterrorism, emergency preparedness, and business continuity, to crime prevention and public health and safety, the VP3 can alert, educate, and engage its members to be actively involved in preparing and protecting themselves, their families, and their communities or organizations against a variety of potential incidents or threats. In addition, VP3 partners become a force multiplier as they lend their informed eyes and ears to the effort to keep their hometowns secure.

For law enforcement, there are several reasons why a broad approach to information-sharing is beneficial. First, an "all-crimes, all-threats, all-hazards" VP3 offers a wider range of potential consumers. This helps to expand the intelligence network and increase the potential range from which data collection can ultimately occur.

Second, attempting to separate crime from terrorism is counterproductive. At its most fundamental level, "crime prevention is terrorism prevention."[10] In fact, many of the same activities that help to prevent crime also help to prevent terrorism. For example, the ability to identify individuals involved in preoperational surveillance, whether for a robbery or an attack on critical infrastructure, involves essentially the same skill set.

Furthermore, the nexus between crime and terrorism has been well-documented. One example is the multi-billion dollar illegal drug trade linked back to Afghanistan that al Qaeda has been able to tap into.[11] In addition, shoplifting, theft, credit card fraud, and document fraud were all activities linked to a Montreal-based terror cell involving Ahmed Ressam, who was arrested for plotting to bomb the Los Angeles International Airport during the millennium celebration.[12] Closer to home, even something as seemingly benign as the illegal sale of cigarettes may be funding terrorist groups such as Hamas, Hezbollah and al Qaeda.[13] All of these crimes may involve, at some point, individuals in our business or residential communities who may be either victims or witnesses to the commission or planning of these crimes. Therefore, by recognizing individuals or circumstances that are suspicious or out of the ordinary, an aware community can help prevent crime and, potentially, terrorist attacks.

Lastly, an "all-hazards" approach facilitates intergovernmental partnerships as a law enforcement agency will likely need to partner with other government agencies and departments in order to gather information for its private sector partners. For instance,

the police department or sheriff's office may partner with the heath department for public health-related information, or the local office of emergency management, which monitors weather and issues advisories. In some metropolitan areas, the transportation department may be the best source for information regarding planned roadwork or unanticipated traffic delays that can affect business continuity. The networking necessary to facilitate the exchange of information between governmental agencies can assist in the overall coordination of effort between these same agencies during exercises, or in the face of a real emergency or catastrophic event.

STARTING WITH A PRIVATE SECURITY PARTNERSHIP

With the pressing homeland security need to protect critical infrastructure, and with most critical infrastructure under private control, private security is a good place for a law enforcement agency to initiate a partnership. In addition, a police-private security partnership can provide a solid platform from which the scope of the VP3 can be expanded at a later point.[14]

Before beginning, getting input into the needs of prospective partners can help set the tone for a successful partnership. Therefore, a police liaison should consider reaching out to local security directors and organizing a meeting to discuss the idea of a partnership before it is launched. The purpose of assembling this group is more than just getting their "buy-in." It is also to learn precisely what a group of knowledgeable and experienced security professionals would like from a partnership. In addition, assembling a meeting of prospective partners can also instill in them a sense of overall responsibility for the system that is eventually created.[15] Research has shown this to be the "most important antecedent of user involvement and attitude toward the system."[16]

In many places, the local chapter of ASIS International, the world's largest organization of security professionals, can serve as a useful umbrella organization and supply obliging partners in helping to organize this type of meeting. This strategy was utilized with great success several years ago in Nassau County, New York in preparation for the launching of the Security/ Police Information Network (SPIN). In this case, an initial meeting to discuss the prospective network firmly established from the beginning that the new initiative was going to be a partnership, and that the views of private sector partners were important.

To facilitate the sharing of information that may be labeled *For Official Use Only* (FOUO), or other sensitive information, an agency should consider vetting its private security directors through an application process. This process will help to create a more trusted environment within the group and, in addition to receiving basic pedigree information, provides the law enforcement agency with an opportunity to obtain details about the responsibilities of the applicant, as well as the number of security and non-security personnel in the company.[17] This information will give the agency better insight into the potential leverage offered by the applicant. For instance, the fact that a security director may have hundreds, or even thousands, of security guards under his authority is information that might be useful to a law enforcement agency. This information could be gleaned from a well-designed application. In addition, if the agency will be administering a secure web-portal (which will be discussed later in this paper) a process for establishing a user name and password must be developed.

Many security professionals enter the field from a law enforcement or military background. In such cases, they are likely to understand the value of good intelligence and information sharing, which affords insight into what type of information may be useful to a law enforcement agency.

After the technological infrastructure and personnel to support the virtual police-private security partnership have been established, agencies can easily expand the network to include neighborhood watch leaders, chambers of commerce, and other community-based organizations. Since an agency will likely share only information meant for wide distribution with these community-based organizations and leaders, a process for vetting members of these groups by conducting background checks may not be necessary. Either way, an application process will enable the agency to know who is on their network.

THE APPLICATION OF INTERNET-BASED TECHNOLOGIES

There are four types of Internet-based technologies that will be examined in terms of facilitating a virtual public-private partnership: email, web portals, web forums, and Groove. In large law enforcement agencies, there may be a place for each of these technologies. Although smaller agencies may not be able to provide the resources needed for every aspect of implementation, some of the concepts and principles that will be discussed may be applied on a smaller scale with the resources that are available.

Email

There are nearly 190 million Americans using email to communicate, making it an inexpensive and timely way to communicate with large numbers of people.[18] With the increasing presence of handheld wireless devices, particularly in the business community, email offers an effective way to deliver timely and actionable information. The presence of computers and internet access in virtually all large businesses and in most homes today provides the tools needed to implement an email-based system. Email allows near instant access to potentially thousands of end users and, equally important, it allows for a direct means of communication back to the agency.

In setting up a system, an agency should attempt to build in maximum flexibility and utility. The greater the ability to select which users receive which information, the better an agency will be in fulfilling the information needs of those on the network. Anticipating future needs is important in designing a system that an agency can grow and expand into.

Some of the types of email messages that may be sent by a VP3 include: robbery notifications, wanted and missing persons notifications, crime stoppers flyers, crime prevention information, homeland security and terrorism-related information, public health related messages, weather alerts, emergency preparedness information, major road closings and delays, disruptions in public transportation, evacuation drills, and weekend events.

In a VP3, email is an important component because it can serve as both a means to deliver content or, as in the case of NYPD Shield, as a means to notify the user that fresh information is available for viewing on a web-portal. It also provides a direct link back to the agency for each user, bringing the law enforcement agency a little closer to each of its private sector partners.

Web Portals

As greater numbers of people rely on the web for information, a web portal becomes increasingly important for a local law enforcement agency. Web portals can provide virtually unlimited access to large numbers of users. Reports and notifications can be archived and links to other agencies and resources can make volumes of information easily accessible.

Keeping the site fresh with regularly updated information that offers value to users is vital to keeping users coming back on a regular basis. In addition, more sophisticated sites are offering content in the form of podcasts or enabling users to sign up for RSS feeds. Such uses of technology typically engage a younger, more technologically savvy demographic.

In developing a web portal, an agency can maintain a public side while creating a members' only section for private security. The public side of the website can be used to post crime-related news, emergency preparedness and public health materials, and other information appropriate for general viewing and consumption. The public side of the web portal should also include a neighborhood watch section with basic crime and terrorism prevention information, giving citizens a sense of their responsibility when it comes to prevention. The New York State Metropolitan Transportation Authority's "If You See Something, Say Something" campaign is an example of this type of information.[19]

A web portal is also a place where the agency can communicate with residents on local issues and problems. The Los Angeles Police Department (LAPD) maintains an outstanding website that allows residents to sign up for E-policing notifications and makes detailed local crime information available for each patrol car area.[20] Local officers routinely write and post a column on the LAPD website, keeping residents informed of the latest crime and disorder problems.

A law enforcement agency can give private security professionals access to more detailed information relating to terrorism and homeland security by maintaining a secure portion on the portal. The opportunity also exists for archiving the Department of Homeland Security Daily Open Source Infrastructure Reports and other important information and intelligence products. The secure, members' only NYPD Shield website provides an excellent example of the type of features that can be built into a web portal tailored for private security professionals.[21]

The number of resources a department can apply to developing a website can vary considerably. In the United Kingdom, for example, police services and constabularies have, for the most part, invested in robust websites that offer outstanding examples for local agencies.[22] Agency heads should understand that investing in a robust website may well be cost-effective if it engages and informs citizens and gives them the information they need to keep themselves and their communities safe.

Web Forums

Web forums have the potential to become virtual communities where people gather online to participate in a community of interest. In some cases, a community of interest may even develop into a community of practice, where people deepen their knowledge and expertise in an area and further the practice by interacting on an ongoing basis.

Research into the areas of virtual communities and social capital suggests that virtual communities tend to increase trust and norms of reciprocity, or social capital, and that a

high level of social capital correlates with low rates of violent crime and safer communities.[23] Consequently, local law enforcement agencies should consider using web forums to facilitate the formation of virtual communities within their respective jurisdictions.

Web forums, which can be made accessible through an agency's web portal, can be open to the public or limited to a certain group of members. For neighborhood watch leaders, agencies should consider making a forum accessible to the general public, as it will allow it to grow by giving those with an interest in crime prevention an opportunity to either join in the discussions or just stand on the sidelines and observe. In such an instance, even though a person may never contribute to the forum, they can still benefit from the information gained.

For private security, vetting participants and limiting access to the forum is very important in creating a trusted environment in which members will share information. In addition, if there is sufficient scale, an agency might consider separate forums for various sectors such as retail, banking, colleges/universities, and hospital security.

For example, in most towns and cities the security personnel working for different department stores have no contact with each other, which works to the advantage of offenders. A forum for retail security, in particular, presents an opportunity for law enforcement agencies to connect the security personnel from various stores throughout their jurisdiction to share general information regarding larceny trends, as well as specific information pertaining to shoplifters.

Whether it is for neighborhood watch or retail store security, a web forum facilitated by a law enforcement agency for private sector partners can enhance public safety and compound the agency's return on investment of resources and personnel for the VP3.

Groove

Microsoft Office Groove offers a potentially powerful tool for providing a secure environment for sharing information. Designed to facilitate collaboration, Groove provides a law enforcement agency the ability to invite specific users into a secure virtual workspace. Because of the relative complexity and the practical limits on the number of individuals who could effectively participate in a workspace, this application could be best utilized for private security directors of critical infrastructure within a jurisdiction. Once invited into a workspace, individuals would be able to share information, conduct discussion threads, and collaborate on documents, all with encryption end-to-end in a secure environment within Groove.[24]

The Illinois State Police has adopted Groove for use agency-wide and has several uses for the collaboration-enabling software.[25] Groove workspaces are created for managing emergencies and assist in the coordination of effort as it synchronizes users and updates the workspace automatically. In addition, the Illinois State Police uses Groove for criminal investigations to enable investigators in different locations in the field to better coordinate by having the latest facts available on a case.[26]

Like a forum, a workspace can potentially spawn a community of practice. Collaborative software, such as Groove, holds great promise for widespread business use as the synergistic fruits of innovation and more efficient and effective practices gained through collaboration represent the competitive advantage for companies in the future. This, in turn, is likely to drive more widespread use in government and law enforcement.

THE VP3 AND THE INTELLIGENCE FUNCTION

Leaders planning to implement a VP3 will need to decide where in the organization to house the partnership. To the extent possible within the logistical constraints of the department, agency heads should approach public-private information sharing with the mindset that a VP3 should be closely tied or integrated into the centralized intelligence function, have real-time access to information regarding the agency's operations, and that, conceptually, data sharing with the private sector should be just an extension of the internal system used to move information within the agency. In larger departments, that may mean that the VP3 should be made part of an intelligence center, where data and crime analysis occurs.

Embedding a VP3 within the centralized intelligence function has many advantages. With information and intelligence readily accessible, both the quality and timeliness of network content will be enhanced. This type of functional consolidation within an intelligence center will streamline the flow of information and dramatically enhance the value that the VP3 offers to private sector consumers. Enhanced value to consumers is likely to result in a more informed and engaged private sector, which is then better able to recognize and, consequently, prevent crime and terrorism.

Intelligence analysis lies at the core of intelligence-led policing, and, as a result, analysts play a critical role in influencing the direction and deployment of police resources. In terms of the 3i Model, analysts do this by *interpreting* the environment and creating intelligence products that can *influence* decision makers. These decision makers, having been influenced by intelligence, can then *impact* the environment.

As discussed earlier, decision makers not only reside within law enforcement, but can also consist of members of the private sector. By keeping the private sector informed and engaged, the criminal environment can be impacted. This is not only anecdotally supported by the community policing experiences of many communities, but is also supported by the limited, but nonetheless empirical evidence gained from the successes of an existing virtual public-private partnership, the Nassau County Security/Police Information Network (SPIN).

Although limited in scope, these successes include two separate bank robbery arrests and an arrest for identity theft.[27] SPIN is also responsible for shutting down a gasoline larceny scheme that had bilked many of Long Island's gas retailers for tens of thousands of dollars each.[28] In every one of these successes, the intelligence network provided by the VP3 was utilized by the law enforcement agency pursuant to an identified intelligence need.

In order for a virtual public-private partnership to be effective, it is vital that the analyst understand his/her responsibility to provide informational products to a variety of consumers, including those in the private sector. This broad responsibility is consistent with a recent directive from the director of national intelligence to move the intelligence community from a "need to know" to a "responsibility to provide" collaborative environment with respect to the private sector.[29] In addition, in terms of the 3i Model, each of these consumers may be a prospective decision maker who can potentially impact the environment.

Instilling a culture that will support information sharing within the agency and with the private sector will be a major factor in determining the success of any partnership. In describing the importance of addressing cultural concerns, David Carter writes:

> One of the greatest weaknesses in the organizational culture of intelligence units is the unwillingness to share information. Police leadership must ensure that intelligence is proactively shared with the people who need the information, both inside the organization and with external agencies. Too many times, intelligence units act as a sponge, absorbing information from diverse sources, but are reluctant to share what they have gathered and learned. This gate-keeping practice is dysfunctional, wastes resources, and contributes to the reluctance of field personnel to submit information.[30]

Establishing an information-sharing policy and guidelines which hold members responsible for delivering information and intelligence products to those who need it can assist in addressing this problem and can help shape the culture of a new VP3. Policies of this type should attempt to balance the need to protect information — that, if released, could jeopardize officer safety or an ongoing investigation — with the need to "provide the right information to the right people at the right time."[31] In addition, policy should direct practices which ensure information assurance and security, as well as compliance with Title 28, Code of Federal Regulations Part 23, concerning the retention of information or intelligence data.[32]

In order to be effective, intelligence must serve the needs of its consumers. Therefore, in order to deliver quality intelligence products to both law enforcement and private sector consumers, analysts should think in terms of several tiers of users, each with different needs. For instance, an analyst may create one version of an intelligence product for law enforcement policy makers, another for general law enforcement, one for private security, and a last version for release to community leaders and the general public.

Although sanitizing products for private sector consumption may sometimes be necessary, it is important to note that many products may be developed exclusively from open source materials. Some, in fact, have suggested that as much as 90 percent of the information available to analysts today is from open sources.[33]

The recent explosion in the growth of the Internet and the development of high-powered search engines has enabled an extraordinary capacity for information collection in the open source domain. The potential value of open source intelligence (OSINT) is increasingly being recognized within the intelligence community. Among the proponents for increasing the exploitation of open sources is Charles E. Allen, assistant secretary for intelligence and analysis for DHS and a forty-nine-year veteran of the IC. Allen seeks to enhance OSINT capacity at DHS through a proposed Domestic Open Source Intelligence Enterprise.[34] As OSINT is increasingly used in intelligence, the mystique and culture of secrecy that enshrouds the IC — and which so many in the community still feed on — will, perhaps, be slowly degraded. As this occurs, local law enforcement intelligence analysts may be more likely to serve a broader consumer base — one that includes private sector customers. Consequently, in the long term, greater exploitation of open sources may have a positive impact on public-private information sharing.

In terms of data collection and intelligence-led policing, it is critical for analysts to understand the extent and the nature of the "expanded" intelligence network provided by a virtual public-private partnership. Although a VP3 can dramatically enhance an agency's capacity to collect information, rather than expending resources collecting massive amounts of information (in the hope of discovering the hidden "pearls" that lie

within), whenever possible the information collection process should be focused and driven by specific information needs.[35]

As analysis identifies intelligence requirements, the VP3 network becomes a means by which law enforcement can access specific segments of the private sector and target collection efforts. Therefore, to realize the potential of a VP3 for enhancing intelligence-led policing, there must be a direct link between identifying intelligence needs and utilizing the VP3's network to fill those needs.

A system that can target data collection for specific segments of the private sector can potentially yield more relevant, hence valuable, information flowing from the private sector into the intelligence cycle. This information, which would not have been available had it not been for the VP3, then feeds into the intelligence cycle, ultimately resulting in better intelligence products. Better intelligence can enable better decisions by consumers of that intelligence, who can then, perhaps, more effectively impact problems in the environment.

Consequently, the potential for the intelligence network to satisfy intelligence requirements increases as more segments of the private sector become part of the network. In other words (generally speaking), the greater the size and broader the scope of the VP3, the greater the potential for filling intelligence needs.

While the ability to target collection is extremely valuable, analysts should not lose sight of the fact that, in terms of dissemination, a VP3's network can potentially reach large numbers of people very quickly. There may be many times when mass dissemination of information is highly desirable in getting the public's assistance in identifying a subject or in solving a crime. In these cases, encouraging wide distribution from network members can engage the "network outside the network" consisting of family and friends.[36] If information is managed effectively, the result can be an extraordinary and unprecedented capacity to disseminate information.

INFORMATION MANAGEMENT

While technology may provide the means by which information is communicated to private sector partners, information management deals with the substance. Managing the content for users is one of the most critical, as well as one of the most difficult, responsibilities in any virtual public-private partnership. To be effective in providing information that has value to users, it is vital that a VP3 determine, to the extent possible, the information needs of its membership.

The VP3 staff, as part of the agency's intelligence function, must coordinate with the agency's crime prevention unit, as well as with other governmental agencies such as health, fire and transportation in order to craft an informational product appropriate for users. Figure 2 shows a VP3 embedded within an Intelligence/Operations Center receiving information from a variety of sources, and subsequently managing that information and delivering it to the private sector.

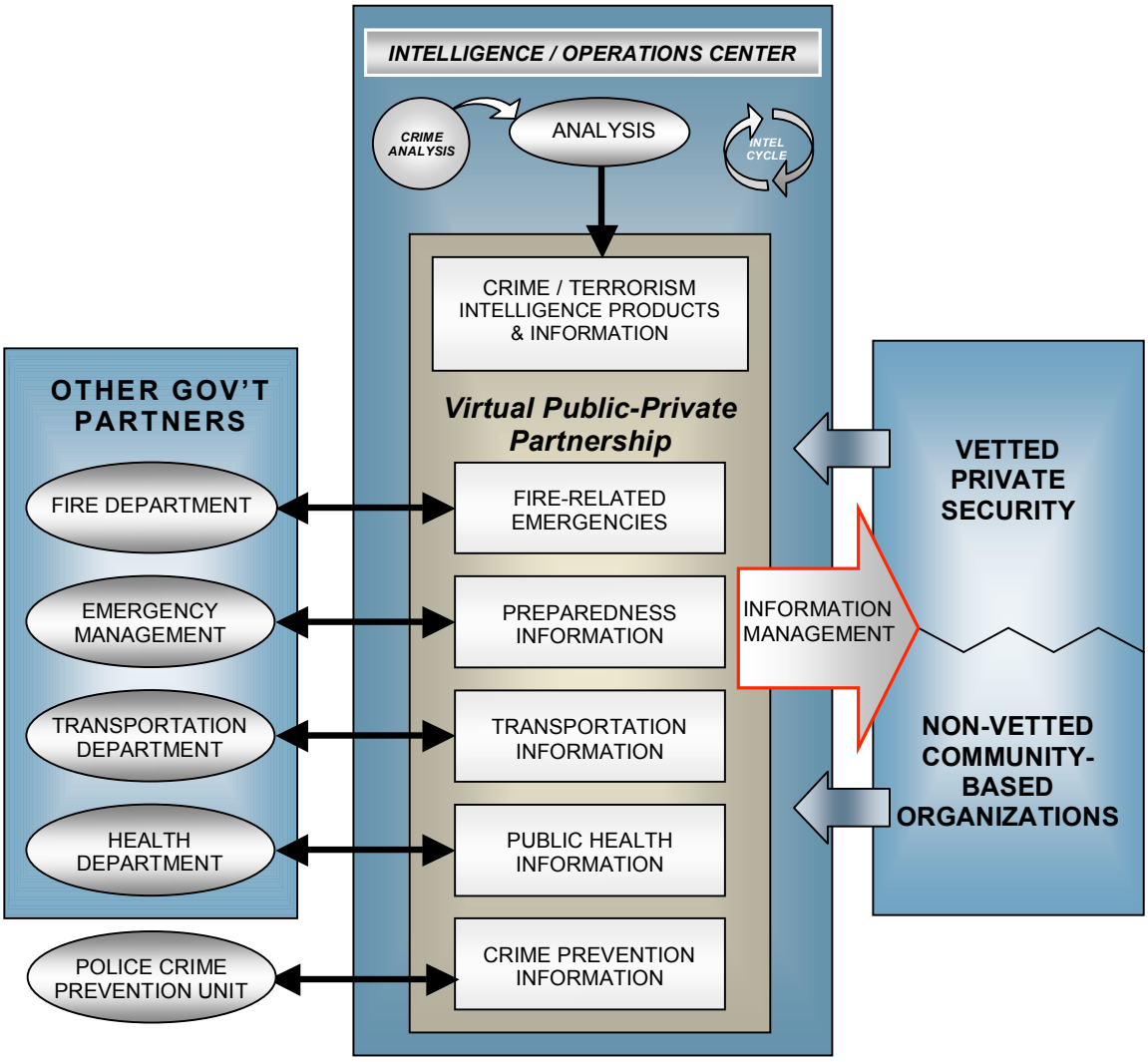

Figure 2. VP3 Information Management.

In terms of an email system, decisions need to be made daily about the type and amount of content that will be sent to each of the many categories of users. Discipline and discretion, in terms of limiting the volume of email to users, must be exercised in order to keep them from disengaging from the network. Those administering the VP3 will want to avoid the possibility of important messages getting lost in the white noise of a flurry of email notifications. This is especially a problem in today's email-laden business environment. Therefore, the more options an agency can give to individual users in deciding what types of messages they would like to receive, the more effective the network can be in its communication. This will help to provide the right balance between too much and too little of the "right" information.

In this regard, a web portal can be of great use. A site can host volumes of information that is available to users at their discretion. For important information, an email could be sent to notify members when important information is posted. In

developing a web portal, to the extent possible, agencies would be well-served in emulating elements found on the web pages of larger agencies such as the NYPD and LAPD, as well as many of the police services of the United Kingdom.

If agencies elect to implement forums or Groove workspaces, they should be monitored daily. The nature of the conversations, or threads, between members could indicate a need for information on the part of the private sector, which could prompt the development of informational product. In addition, as was discussed earlier, as the amount of data in a forum increases over time, the agency might pursue employing a keyword search engine to enable the mining of potentially valuable information.

In terms of network content, informing and educating partners will better enable them to recognize suspicious activities and precursors to crime and terrorism. For example, a "large number of males using a rented apartment irregularly," or unusual chemical odors emanating from a house or apartment, are types of suspicious activities or behavior that should be reported to law enforcement.[37] In addition, as discussed earlier, precursor crimes to terrorism can range from selling counterfeit cigarettes, CDs, DVDs, and handbags, to illegal drug sales, credit card theft, money laundering, and cyberfraud.[38] Including information such as this in VP3 training material can help to demonstrate to members the breadth of criminal activities that may be involved in funding terrorism. It can also help reinforce the important role the private sector can play in keeping our hometowns safe.

The Right to Privacy and Concerns of Domestic Surveillance

It is important to note here that in implementing a VP3, law enforcement agencies need to be ever cognizant of the issue of civil liberties. Concerns of "domestic surveillance" can arise if citizens are asked, in effect, to "spy" on fellow citizens, or encouraged to gather and report information to law enforcement which would otherwise be constitutionally protected. Even if the network is used appropriately and accusations involving the violation of citizens' rights are unwarranted, community perceptions which are negative and pervasive will likely be enough to thwart the overall effort. These perceptions are very much tied to the level of trust conferred by citizens on their police, which is the very foundation upon which citizens extend to government their consent to be policed.

Therefore, agencies must administer the VP3 in a way that not only respects the constitutional right to privacy of individuals, but also engenders trust in the communities those agencies serve. This can be facilitated through careful oversight and management of network content, and by strict adherence to Title 28, Code of Federal Regulations Part 23, concerning the retention of information or intelligence data.[39]

Equally important, law enforcement agencies must build trust in their everyday dealings with citizens. In this regard, trust in the VP3 will likely be a function of the overall level of trust between the individual department and the citizens it serves. Accordingly, agencies that enjoy high-trust relations with their various communities will likely have a greater chance of success in implementing VP3s than agencies which consistently violate the public trust.

The Value of Crime Data

Having discussed the importance and value of a VP3 being closely linked to the intelligence function, it should be noted that linking the partnership to the availability of

timely crime data can also offer great value. Statistics such as the latest crime trends and patterns can be particularly useful to chambers of commerce and neighborhood watch groups. For those agencies that have implemented a COMPSTAT model, the very timely and accurate crime data that results from that process can be valuable to private sector partners as agencies can involve members of the business or residential community in the problem-solving process.

Moreover, the opportunity exists here to tailor crime prevention information to meet the specific need. Distributing or otherwise making these materials available to the network will enable communities to better protect themselves. This type of proactive approach to crime prevention can enhance the effectiveness of the partnership by yielding positive results in reducing overall crime.

Keeping community and neighborhood watch leaders informed also facilitates community organization and participation. The content shared through the network gives these local leaders a direction and purpose to meet or form their own virtual networks at the neighborhood level. In terms of public safety, this kind of leverage can significantly compound the law enforcement agency's return on investment.

NETWORKING

In addition to managing the technology and the content involved in administering a VP3, another important component of the partnership involves networking. David E. Dial, in his work "Enterprise Policing for the September 12 Era," describes a form of policing that involves "networking in unprecedented ways with other law enforcement and government agencies, as well as community members."[40] In terms of Dial's Enterprise Policing model, the importance of networking for law enforcement agencies cannot be overstated. Dial goes on to write:

> Police agencies that fail in their efforts to develop networks and information sharing capabilities with other government and private-sector agencies might find themselves suffering from linkage blindness. The lack of networking and information sharing can result in failure to predict terrorist activity.[41]

This gap between local law enforcement agencies and the private sector presently exists on a broad scale and is a strategic weak point in our nation's homeland security. A VP3 can be the mechanism by which a law enforcement agency closes that gap by developing a type of expansive network that, just a few years ago, was not technically feasible.

As was discussed earlier, administering an "all-crimes, all-threats, all-hazards" network will require coordination and information sharing with other governmental departments. The VP3 staff, therefore, will need to build relationships with members of these other agencies such as fire, emergency management, transportation, and health. This will require deft interpersonal skills, as well as an awareness and understanding of the political environment. It may also require the assistance of the agency head to garner support for the initiative at the top levels of the other governmental agencies involved.

In terms of connecting with the private sector, identifying umbrella organizations within segments of the business community and attempting to bring their membership into the network is the most efficient and effective way of reaching large numbers of potential members with minimal personnel resources. This will likely require presentations at the meetings of those organizations. Therefore a big part of growing the

network involves getting out into the various communities in order to involve them in the VP3. For example, in developing SPIN, the Nassau County Police Department leveraged a wide range of organizations, the scope of which was a contributing factor to success.[42]

As a partnership grows and various segments of the private sector become connected, the enormous potential of the network becomes evident. Having direct links with a vast array of organizations and communities, and having their members as part of the network, offers law enforcement agencies exponential gains in the capacity for data dissemination and collection. When weighed against the number of staff required for implementation, an analysis of the long-term impact that a VP3 network can have on the entire policing operation will likely find that investment to be extremely cost-effective.

In time, as an increasing number of agencies develop VP3s and begin to network and share information with each other, they can take advantage of the VP3 resources of other agencies. This has begun to occur between agencies in the New York Metropolitan area as NYPD Shield, Nassau County SPIN, and the Suffolk County Alert Network (SCAN) have begun sharing information and resources with each other.

MEETINGS

Live meetings can add tremendous value to any law enforcement-administered virtual public-private partnership. In addition to providing a forum for presenting important and timely information, they also provide an opportunity for feedback and to celebrate any network successes. Meetings also reinforce the sense of community between the individuals in the network by providing an opportunity for networking and developing relationships between themselves and with the staff of the law enforcement agency.

With differences in roles and responsibilities, and consequently differences in the need for information, the meetings for private security and community-based leaders should be conducted separately. From the perspective of private security leaders, conducting separate meetings is also symbolic in that it acknowledges the important contribution to public safety and homeland security that stems from their security responsibilities, especially with regard to critical infrastructure.

There is another reason why an agency might want to conduct face-to-face meetings with members of a VP3. As stated before, researchers have found that virtual communities tend to increase trust and norms of reciprocity, or social capital. Findings also suggest, however, that this effect on social capital is greatest when the face-to-face network overlaps with the virtual network.[43] In addition, social capital should increase when opportunities for civic engagement are facilitated in physically-based virtual communities, as would be the case in a VP3 administered by a local law enforcement agency.[44] Additionally, higher levels of social capital are shown to be positively correlated to lower rates of crime.[45]

Moreover, with respect to civic engagement, a 2002 study found that there are three factors that contribute to increased civic engagement: motivation, skills, and network connections.[46] Therefore, by networking private sector partners through technology, and by holding live meetings in which these partners are motivated, given knowledge and skills, and then presented with opportunities for civic engagement, members of the

VP3 may be more likely to contribute to community safety. In this way, citizens are used as a force multiplier.

Law enforcement agencies should, therefore, be prepared to inform citizens of how they may assist police and be of service to their communities and their nation. Citizens can be directed towards a number of volunteer efforts, such as Citizen Corps, which consists of programs such as Community Emergency Response Team (CERT) and Volunteers in Police Service and Neighborhood Watch. In some parts of the nation, law enforcement agencies oversee voluntary auxiliary police forces that, in essence, act as eyes and ears for the police and assist in traffic-related duties.

Meetings, therefore, are an important part of any virtual public-private partnership. Unlike most virtual communities, which are geographically dispersed, a VP3 administered by a local law enforcement agency is based in and around an agency's jurisdiction, providing a valuable opportunity upon which departments should take full advantage.

CREATING A CULTURE OF PREPAREDNESS

In February 2006, the White House released *The Federal Response to Hurricane Katrina: Lessons Learned*, which recognized that everyone, from private citizens to the federal government, has a role to play in homeland security. [47] The report called for a continuing transformation for homeland security that will be "the most profound and enduring — the creation of a Culture of Preparedness."[48]

By keeping partners abreast of "all-hazards" issues, an agency administering a VP3 can help create awareness in its members of the need to be prepared. It is this awareness that is the first step in getting citizens to take actions that will better prepare themselves, their families, and their communities for unforeseen events and emergencies.

Although creating a culture of preparedness may be best coordinated and organized at the federal level, which can expend the resources necessary to develop and produce an effective advertising campaign, delivering the message is best done locally. In building a robust network that reaches deeply into the private sector, a local law enforcement agency creates the means by which preparedness campaign messages can be delivered. With the powerful connectivity that comes with networking community-based organizations, large portions of the business community, and a large and ever-growing private security community, the agency can assist in helping to create a culture of preparedness and introduce members to the U.S. Department of Homeland Security's preparedness website, Ready.gov.

At this site one can find information on The Ready Campaign, which consists of Ready America, Ready Business, and Ready Kids. The site also has easy links to public service announcements, brochures that can be easily downloaded, and information that effectively communicates a message of preparedness.[49] The campaign's tagline is "Prepare, Plan, Stay Informed."

The campaign's public service announcements were produced by the Department of Homeland Security in conjunction with the Advertising Council and are very well produced. Unfortunately, these short videos only run on donated airtime and, consequently, do not receive much exposure. A VP3 provides an excellent venue for a monthly preparedness message that can consist of an email with embedded hyperlinks

to preparedness videos and attached brochures, as well as enabling access via a preparedness page on the agency's web-portal.

Educating a nation and transforming its culture is a long-term effort that will take many years. A VP3 can provide an effective way to support the national effort to prepare America by delivering information that engages citizens, making them more aware of their environment, and then challenging them to be prepared for worst-case scenarios.

CONCLUSION

During the past decade, the growth of the Internet has been utterly explosive. Its development has exponentially increased the capacity to communicate, which has led to globalization and has moved society squarely into "the information age." It has enabled companies to make quantum leaps in their ability to access and transmit information. The effect on commerce has been, in a word, transformational.

Ten years ago, it was market forces combined with the extraordinary capacity to move information and instantly connect people that made the large-scale adoption of the Internet by the business community inevitable. The technology filled a need and offered advantages which companies needed to leverage if they wanted to remain competitive.

Although law enforcement is not driven by the profit motive, policing is, in many ways, an information business. In order to remain competitive in the business of fighting crime and maintaining safe communities, law enforcement agencies are beginning to move towards intelligence-led policing, which relies on information to paint the best possible picture of the criminal environment.

Much of the justification for implementing virtual public-private partnerships rests on the case presented in this paper that the majority of the information needed by local law enforcement to solve crimes resides within the private sector. To support this, it was noted that there is, on average, only one officer per every 400 residents in the United States. At this ratio, it is apparent that law enforcement would be able to solve relatively few crimes without the cooperation of victims and witnesses. The television show *America's Most Wanted* was offered as an example of the fact that criminals live and work in our communities and that technology can enable law enforcement to deliver information to citizens that can lead to the capture of those wanted persons.

Also supporting the argument for VP3s is the fact is that private security makes up nearly three-quarters of the protective workforce and that the vast majority of critical infrastructure is under private control. Therefore, private security firms, it was noted, are perhaps in the best position to be "first preventers" of crime and terrorism.

In many ways, the question of whether the large scale adoption of VP3s will occur within local law enforcement agencies in the United States may be analogous to the question twenty-five years ago asking whether law enforcement agencies will someday utilize computers in everyday policing. The enhanced level of effectiveness in fighting crime that was made possible by computers was the driving force behind their eventual widespread adoption. It is this same rationale that will, perhaps drive agencies towards implementing VP3s. If the private sector offers the value to local law enforcement that has been suggested in this paper, and technology offers a free way to network agencies with key private sector entities in their communities, the move towards the adoption of VP3s, like that of computers in policing, may be inevitable.

As criminals and terrorists have become increasingly networked and have leveraged the Internet to achieve an unprecedented capacity to plan and conduct their criminal enterprises and operations, local law enforcement agencies must do the same in order to keep their communities safe. Until now, however, the extent of networking has been limited. Since 9/11, local law enforcement agencies have made tremendous gains in terms of networking themselves with federal, state, and other local law enforcement agencies, but have not made nearly the same level of progress in networking themselves with the private sector. Virtual public-private partnerships can offer tremendous leverage in accomplishing this.

Earlier in this paper it was suggested that America may need to develop an alternative strategy to deal with the extraordinary costs related to responding to the threat of terrorism. The adoption of VP3s by local law enforcement agencies may be an effective alternative strategy. The adoption of VP3s, however, is not likely to occur until it becomes apparent to local police chiefs and sheriffs that the effort to do so is cost beneficial and, in fact, leads to safer communities and lower rates of crime. This paper attempts to provide such evidence and, in doing so, offers a VP3-enhanced model of intelligence-led policing (see Figure 3).

Although building vast VP3 networks via the Internet has extraordinary utility, the enduring value lies in the byproduct of such systems. In the end, it is changed behavior that a police department seeks. Through information sharing, a law enforcement agency can educate members of the community, build social capital and trust and, as a result, increase the propensity of individuals to report suspicious behavior. This is the environment that can help bring about the one phone call from a concerned citizen that may help prevent the next terrorist attack. By engaging citizens and involving them in the issues that affect their communities, keeping them informed about what is happening where they live or work, and then allowing them to network between themselves, internet technology can be used to leverage the private sector as both a force multiplier and a vast potential source of information.

The lesson learned from two decades of community policing — that citizens play an important role in helping to maintain their own safe neighborhoods — also applies to the realm of hometown and homeland security. If the United States is to survive this age of the terrorist threat, American society must adapt and its citizens must share responsibility for homeland security. Virtual public-private partnerships can play a major role in accomplishing that. In implementing a VP3, a local law enforcement agency will not only enhance its intelligence-led policing capacity, but can ultimately achieve greater levels of public safety and homeland security.

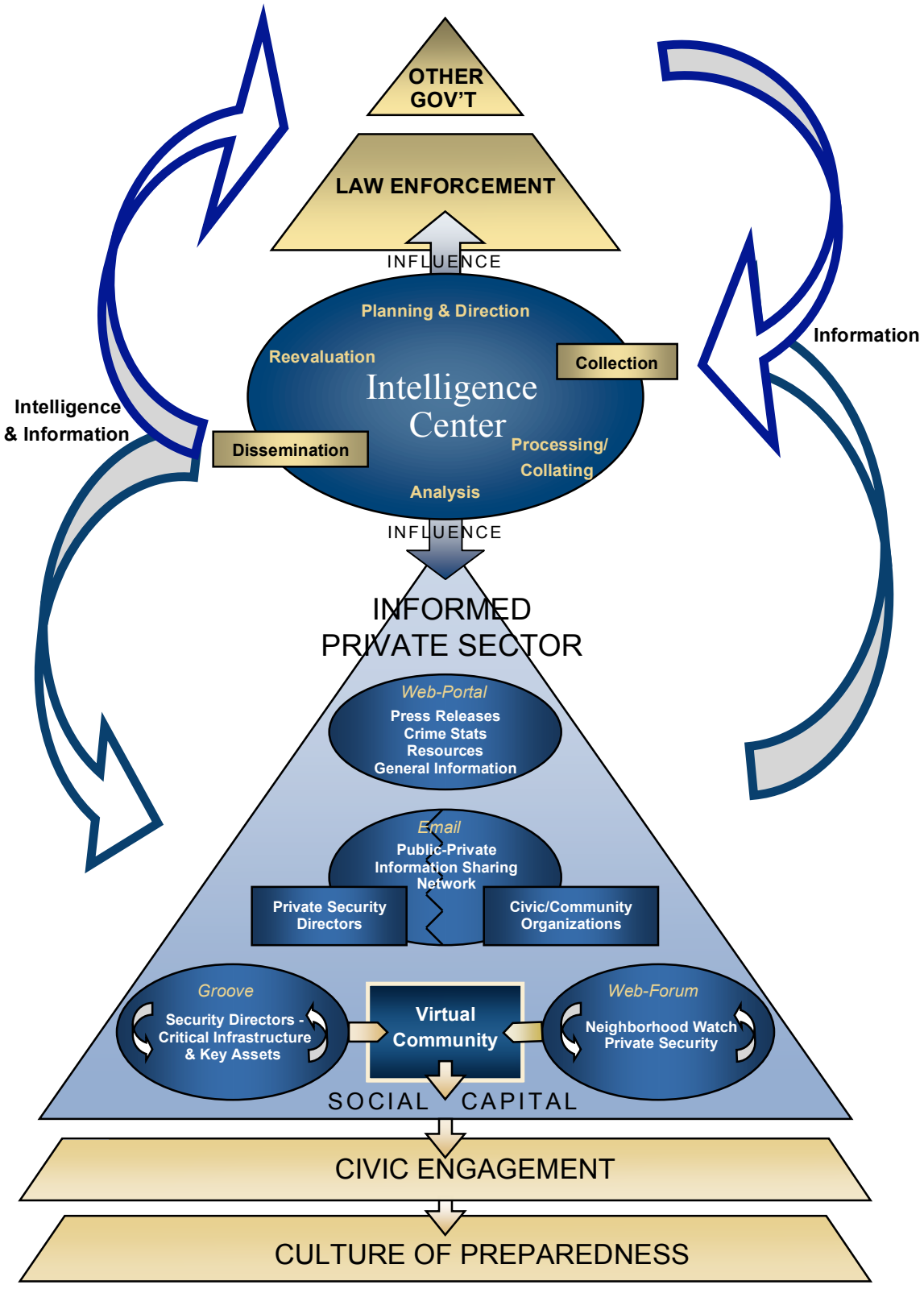

Figure 3. A VP3-Enhanced Intelligence-Led Policing Model.

Inspector Matthew J. Simeone, Jr. is a twenty-two-year veteran of the Nassau County Police Department who is presently assigned as the county's Task Force Against Gangs coordinator and commanding officer of community affairs. In 2004, he created the Nassau County Police Department's Security/Police Information Network (SPIN), a virtual public-private information sharing partnership. Inspector Simeone is a graduate of the Naval Postgraduate School's Center for Homeland Defense and Security, where he earned a master's degree in homeland security. He is also an alumnus of the 210th session of the FBI National Academy.

---

[1] Department of Homeland Security, *Overview: FY2007 Homeland Security Grant Program* (Washington DC: U.S. Department of Homeland Security, January 2007), 2, http://www.ojp.usdoj.gov/odp/docs/fy07_hsgp_overview.pdf. In FY2007 alone, over 1.25 billion dollars was budgeted for the Urban Areas Security Initiative ($746.9 million) and the State Homeland Security Program ($509.2 million).

[2] International Association of Chiefs of Police, Community Oriented Policing Services, *Private Security/Public Policing*, *Vital Issues and Policy Recommendations* (Washington, DC: U.S. Department of Justice, 2004), 3, http://www.cops.usdoj.gov/mime/open.pdf?Item=1355.

[3] Brian A. Reaves, *Census of State and Local Law Enforcement Agencies, 2004* (Washington DC, Bureau of Justice Statistics, June 2007), 3, http://www.ojp.usdoj.gov/bjs/pub/pdf/csllea04.pdf. One officer per 400 residents was extrapolated from this census, which documented an average of 249 sworn State and local officers per 100,000 population.

[4] *Private Security/Public Policing*, *Vital Issues*, 2; William C. Cunningham, "U.S. Private Security Trends," Presentation (Amelia Island: Hallcrest Systems, February 2003), 4.

[5] http://www.internetworldstats.com/top25.htm. Internet World Stats, using data from Nielsen/NetRatings, reports that 69.7% of Americans use the internet.

[6] Jerry H. Ratcliffe, "Intelligence-Led Policing," *Australian Institute of Criminology, Trends & Issues in Crime and Criminal Justice*, no. 248 (April 2003): 3. http://www.aic.gov.au/publications/tandi/ti248.pdf.

[7] Ibid, 4.

[8] NYPD Shield website, http://www.nypdshield.org/public/.

[9] Nassau County Police Department SPIN webpage, http://www.police.co.nassau.ny.us/SPIN/spininfo.htm; Suffolk County SCAN webpage, http://www.co.suffolk.ny.us/police/scan.htm.

[10] Sheriff Larry Campbell, Leon County, Florida, as quoted in "Crime Prevention Can Spur and Support Homeland Security in Neighborhoods and Communities," *Topics in Crime Prevention,* National Crime Prevention Council (Winter 2003): 1, http://www.ncpc.org/cms/cms-upload/ncpc/File/topics_cp_hs.pdf.

[11] Tim McGirk, "Terrorism's Harvest," *Time*, August 9, 2004, 41; Elaine Shannon, "The New War on Afghan Heroin," *Time*, November 25, 2002, 23.

[12] Dr. Louise I. Shelley, John T. Picarelli, Allison Irby, Douglas M. Hart, Patricia A. Craig-Hart, Dr. Phil Williams, Steven Simon, Nabi Abdullaev, Bartosz Stanislawski, and Laura Covill, "Methods and Motives: Exploring Links Between Transnational Organized Crime & International Terrorism," September 2005, 40, http://www.ncjrs.gov/pdffiles1/nij/grants/211207.pdf.

[13] Sari Horowitz, "Cigarette Smuggling Linked to Terrorism," *Washington Post*, June 8, 2004.

[14] Cunningham, "U.S. Private Security Trends," 4.

[15] Jon Hartwick and Henri Barki, "Explaining the Role of User Participation in Information System Use," *Management Science* 40, no. 4 (April 1994): 457.

[16] Ibid.

[17] *SPIN Application*, Nassau County Police Department website.

[18] "How Men and Women Use the Internet," *Pew Internet & American Life Project* (Washington DC: December 28, 2005), ii, http://www.pewinternet.org/pdfs/PIP_Women_and_Men_online.pdf. This report states that 94% of online women and 88% of online men use the internet. Nielsen/NetRatings reported the number of online users in the United States at 210,080,067 in November 2006 according to Internet World Stats at http://www.internetworldstats.com/top25.htm.

[19] New York State MTA, "If You See Something, Say Something" Campaign. http://www.mta.info/mta/security/index.html.

[20] Los Angeles Police Department website, http://www.lapdonline.org/e_policing.

[21] NYPD Shield Website.

[22] Any of the fifty-two U.K. policing agencies can be easily accessed by logging on to http://www.police.uk/forces.htm. Once there, clicking on geographic regions of the map will enable access to the individual websites of local agencies in that region.

[23] Anita Blanchard and Tom Horan, "Virtual Communities and Social Capital," *Social Science Computer Review* 16, no. 3 (Fall 1998): 293, http://www.idea-group.com/downloads/excerpts/garson.pdf; Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon & Schuster, 2000): 308; Susan Saegert, Gary Winkel, and Charles Swartz, "Social Capital and Crime in New York City's Low Income Housing," *Housing Policy Debate* 13, no. 1 (2002): 218. http://fanniemaefoundation.org/programs/hpd/pdf/hpd_1301_saegert.pdf.

[24] Microsoft, *Groove Product Guide* (September 2006), 2, 8, http://office.microsoft.com/en-us/groove/HA101680011033.aspx.

[25] Interview with Inspector Kevin D. Eack, Senior Terrorism Advisor, Illinois State Police, August 22, 2007.

[26] Ibid.

[27] Interview with Detective Sergeant William M. Leahy, Nassau County Police Department Security/Police Information Network, August 6, 2007.

[28] Oksana Farber, "Positive SPIN on Liaisons," *Security Management* 50 (June 2006), 110.

[29] Michael McConnell, "United States Intelligence Community 100 Day Plan for Integration and Collaboration," 9, http://fas.org/irp/dni/100-day-plan.pdf.

[30] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Washington, DC: Office of Community Oriented Policing Services, November 2004); *National Criminal Intelligence Sharing Plan*, 62, http://www.fas.org/irp/agency/doj/lei/guide.pdf.

[31] Robert S. Mueller III, Director, Federal Bureau of Investigation, "Address to U.S. Chamber of Commerce, Washington, DC, January 19, 2006," *Vital Speeches of the Day,* 72, Issue 9 (February 15, 2006): 258. http://proquest.umi.com.libproxy.nps.edu/pqdweb?index=4&sid=2&srchmode=1&vinst=PROD&fmt=6&startpage=-1&clientid=11969&vname=PQD&RQT=309&did=1034268181&scaling=FULL&ts=1187536507&vtype=PQD&rqt=309&TS=1187536521&clientId=11969.

[32] Title 28 Code of Federal Regulations (CFR) Part 23, *Criminal Intelligence Systems Operating Policies*. http://a257.g.akamaitech.net/7/257/2422/01jul20061500/edocket.access.gpo.gov/cfr_2006/julqtr/pdf/28cfr23.20.pdf.

[33] Statement by Lieutenant General Sam Wilson, USA Ret. former Director, Defense Intelligence Agency, reported by David Reed, "Aspiring to Spying," *The Washington Times,* Regional News, November 14, 1997, 1: "Ninety percent of intelligence comes from open sources. The other 10 percent, the clandestine work, is just the most dramatic. The real intelligence hero is Sherlock Holmes, not James Bond."

[34] Charles E. Allen, Assistant Secretary, *Statement to the Subcommittee on Intelligence Information Sharing and Terrorism Risk Assessment*, House Homeland Security Committee, February 14, 2007. Available online: http://www.fas.org/irp/congress/2007_hr/021407allen.pdf.

[35] Carter, *Law Enforcement Intelligence: Guide*, 148.

[36] Interview with Detective Sergeant William M. Leahy.

[37] George L. Kelling, William J. Bratton, "Policing Terrorism," *Civic Bulletin*, no. 43 (Center for Civic Innovation at the Manhattan Institute, 2006), 4, http://www.manhattan-institute.org/pdf/cb_43.pdf.

[38] Sari Horwitz, "Cigarette Smuggling Linked to Terrorism," *Washington Post*, June 8, 2004; Troy Anderson, "Drug Sales, Counterfeiting Funding Terrorism," *LA Daily News,* August 19, 2007; Jon Swartz, *USA Today*, February 20, 2005.

[39] Title 28, Code of Federal Regulations(CFR) Part 23, *Criminal Intelligence Systems Operating Policies* at http://a257.g.akamaitech.net/7/257/2422/01jul20061500/edocket.access.gpo.gov/cfr_2006/julqtr/pdf/28cfr23.20.pdf.

[40] David E. Dial, "Enterprise Policing for the September 12 Era" (master's thesis, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, March 2006), v. https://www.hsdl.org/homesec/docs/theses/06Mar_Dial.pdf.

[41] Ibid., 41. Dial refers to "linkage blindness," a term coined by Steven A. Egger, *Killers Among Us,* 2nd ed. (Upper Saddle River, NJ: Prentice Hall, 2002), 251-258. Linkage blindness refers to a failure to share or coordinate investigative information and a lack of adequate networking among law enforcement officers.

[42] The following organizations were leveraged by the Nassau County Police Department in developing SPIN: ASIS International Long Island Chapter, the Long Island College and University Security Consortium, the International Hospital Association of Security Services, the Long Island Fraud and Forgery Association, the Long Island Gasoline Retailers Association, the Long Island Defense Contractors, the International Petroleum Association, the American Chemistry Council, InfraGard, the Contingency Planning Exchange, the Nassau County Association of Water Districts, the Long Island Import Export Association, the Nassau County Chambers of Commerce, the Retail Loss Prevention Information Network, the Jeweler's Security Alliance, the National Association of Chain Drug Stores, Rx Patrol, the New York State Self Storage Association, the Nassau County Medical Society, the Long Island Forum for Technology, and the Nassau/Suffolk Boards of Education.

[43] Blanchard et al., "Virtual Communities and Social Capital," 293.

[44] Ibid.

[45] Putnam, *Bowling Alone: The Collapse and Revival of American Community*, 308; Saegert et al., "Social Capital and Crime in New York City's Low Income Housing," 218.

[46] John J. Kirlin and Mary K. Kirlin, "Strengthening Effective Government-Citizen Connections through Greater Civic Engagement," *Public Administration Review* (September 2002): 80, http://proquest.umi.com.libproxy.nps.edu/pqdweb?sid=3&vinst=PROD&fmt=6&startpage=-1&clientid=11969&vname=PQD&RQT=309&did=156494601&scaling=FULL&vtype=PQD&rqt=309&TS=1187907624&clientId=11969.

[47] White House Report, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, DC: February 2006), 79, http://www.whitehouse.gov/reports/katrina-lessons-learned/.

[48] Ibid.

[49] "The Ready Campaign," *Ready.gov* website.