Intelligence *Forward*.
Thinking (and Seeing) Ahead

By

Mark R. DuPont

Senior Intelligence and Domestic Security Officer

Florida FWC Division of Law Enforcement

CWO3 (ret) USCGR

I. Purpose

Intelligence is a function of homeland security and law enforcement. It is a subject that you have heard mentioned and talked about over and over again in the aftermath of 9-11. From the 9-11 Commission Report which stated the following;

> "*"Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility, but also responsibility so poorly defined or so ambiguously delegated that action gets lost*." That comment was made more that 40 years ago, about Pearl Harbor. We hope another commission, writing in the future about another attack, does not again find this quotation to be so apt."
>
> The document goes further to state that the "biggest impediment to all-source analysis-to a greater likelihood of connecting the dots-is the human or systematic resistance to sharing information."

This mention of Peal Harbor and of the human element are key elements and will be discussed in detail further in this paper. That human element is what I think we are losing focus of, in the quest for more and more information. For some reason, we are getting caught in the trap that many before us have fallen into.

Our intelligence system appears flawed. It is what many point to as a fault for what happened, and what many others point to today as having to fix. And the "fix" that we as a country are trying to conduct is producing many dollars in grants and budget line items, many jobs throughout the defense and law enforcement communities, and many fusion centers as the silver bullet that will prevent a thing like 9-11 from ever happening on our soil again.

Let me be clear: those things are all important as we strive to increase the likelihood of detection, but if that is where we focus we are missing a key ingredient. Intelligence is also a thing that most people don't understand… even though they think they do. From the common citizen that hears the term digested on the evening news, to the law enforcement professional assigned the duties of intelligence, to the supervisors and leaders that they work for and answer to, many do not fully understand what it is and what it isn't. That, in and of itself, makes it difficult to solve the problem.

Consider this analogy: Your police chief has just been delegated the responsibility for all surgeries that occur at the local hospital, and is therefore putting together the processes to ensure that it all improves and fewer people die in the operating room. Oh, I'm sure that there are people out there that will do a pretty good job at it, but the reality is that they will not know what they don't know.

Building an intel program has similar obstacles, especially for those that think they know or are applying old methods and solutions to the current problem. In the words of Einstein, *"You can never solve a problem on the level on which it was created."*

Well, with that all said, I've got good news and I've got bad news…. Which would you like first? To keep your attention, I'll start with the thorns and obstacles in the path we're on now, and end with a detour that might get us to the end goal faster, and safer.

We'll look at how intelligence programs are being built, and we'll even look back in time to see what intelligence gave us and what we failed to do, and try to figure out why. I guarantee if you follow along to the end of the paper, I will get you to at least look outside your box (paradigm), if not think outside it, in order to improve and enhance your chance for success and the security of the place we call our homeland. And I will keep it simple, I promise.

I have the answer, the silver bullet if you will. The ultimate sensor that you can turn on today and begin collecting critical intelligence tomorrow.

II. Definition

Just for clarification early on in this discussion, (bear with me for a moment, even though many of you reading may know what it is) I want to define Intelligence. According to the publication *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*,

> Intelligence is *an information product of an analytic process*, needed by law enforcement officers and our leaders, in order to keep our citizens and our resources safe from harm. Intelligence is preventative, related to threats of terrorism or crime by using information to apprehend offenders, harden targets, and eliminate or mitigate the threat. Otherwise know as "tactical" intelligence. Intelligence provides decision makers information about the changing nature of threats in order to develop response strategies and reallocation of resources. This is "strategic" intelligence.

The key part of the discussion is the four key words of the definition: Information Product of an Analytical Process. Let's break out each one of the cornerstones of Intelligence.

A. Information

This is pretty simple. Intelligence is and equals information, in part but not in whole. The basic foundation of an intelligence program is the collection and dissemination of that information. Who has it and how do I get it? That is the essence of the intelligence function.

Key point here: Intelligence is NOT pieces of information about people, places, or events that can be used to provide insight about criminality or crime threats.[1] That is just raw

[1] Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies, 2003

data. I said that Intelligence = Information, but not just the information on its own. See next paragraph for further definition.

B. Product

Intelligence is an information *product*, which means something was created from the raw data. Someone, somewhere, took that raw data and did something to it. Knowing that John Smith was at the address of Frank Jones last night is not intelligence, it's information. Knowing that Frank Jones is an illegal alien, currently using an alias and connected to a terrorist organization in the Caribbean, while John Smith is being observed by the FBI and suspected of planning an attack on a cruise ship…now THAT is intel. So what's the difference? How was this "product" created? See below.

C. Analytical

The raw information must be analyzed. Someone who has access to lots of different pieces of information needs to connect the dots. Is there a piece of data that when connected to something seemingly unrelated, gives indications that a crime or illicit act might be created? Intelligence is created when a wide array of raw information is assessed for validity and reliability, and given meaning through the application of inductive and deductive logic. Key point here is that you can't buy inductive and deductive logic. There is no technology out there that will reproduce that for you, but I am jumping ahead. How do we make sure that the information gets to the right place so that it can be analyzed and an output produced? See below.

D. Process

You have to have a process by which information can flow through the right channels, get to the place to where someone can connect the dots, and a means by which that product can get in the hands of the war fighters who can prevent it from happening. Intelligence is the **product** of an **analytical** *process* that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats

and conditions associated with criminality. It is arriving at something more than was evident before.[2]

In my opinion, that is a key part, key ingredient of any intelligence program. If your process does not allow you to arrive at something that you wouldn't see otherwise, you don't have an intelligence program. At best, you have a sorry excuse for information sharing. Notice I said, at best.

The question surrounding the effectiveness of your intelligence program, whether you are the intelligence officer, a senior official, part of the command cadre or just the officer on the street, is this: who has the information and how do I get it?

III. Intelligence as a System

The answer to the question asked in the previous paragraph rests here. The system is the parameters by which information will flow, upward and downward within your department or agency, horizontally and vertically to partners on the federal, state and local level. It provides guidelines for those within to follow, assuring that there is timely delivery, limited duplicity, connecting of the dots, and most importantly, feedback to the field operatives that provided it.

Timely delivery means that the guy or gal in the field who encounters something that could be of value, has the ability and/or tool to get that information to those that can look at it and connect the dots. Timely delivery also means dissemination of that information to the people that need it.

Limited duplicity means that in this era of information overload, we have the means of vetting and filtering that flow. Rather than the officer sending that piece of information to

[2] International Association of Law Enforcement Intelligence Analysts

700 other officers, it goes to one central location that can analyze and disseminate to those that need the information.

Connecting the dots is the analysis process of the data that flows. Somewhere in the system, someone has to stop and take a close look at it. The process has to allow that moment in time where someone uses training, experience, and knowledge to say "this is important. This is connected to something greater or bigger."

Feedback is the key ingredient. To that officer that provided that piece of information, you need to respond back and let him or her know that what he or she provided was a vital link to a very large threat, or that it wasn't. Either way, let them know that you are taking their information and acting on it. It's the one and only way you can insure you get information, and *continue* to get it.

IV. How to build the System

Not that this is the only way to build an Intelligence System within your agency or department, but it seems to have some value hear in Florida for the agency I work for. It's easy to understand and it has a graphic that everyone can understand. (We all love pictures, I know, I know.)

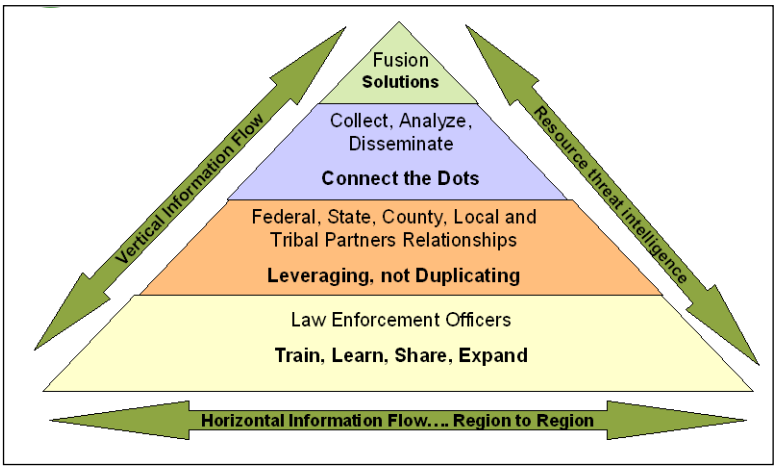
A. The Foundation

Each component in your system represents a block in the pyramid. And when you build a pyramid, or anything for that matter, you can never start at the top. You can't start building your house by putting the roof on; you have to start with a foundation. And the strength of that foundation will determine the life of that project, if it will stand the elements around it, if it will stand the test of time.

For us and for you, that foundation is the foundation of our agency: our officers in the field. They are the basis by which we need to establish a plan. If we focus on having a

great intel officer in the agency, with no connectivity to the field, our program isn't going to get too far. Our pyramid will come tumbling down pretty quickly. Not only are the officers the foundation, they are the eyes and ears with unique abilities and knowledge about what is right and what is wrong out there on the streets, on the water or in the woods. This is the essence of the Community Oriented Policing doctrine. They have the pulse on their domain and are the only ones who can detect an anomaly.

So how do you insure the strength of your foundation? You give them the **training** on how and what to do in the intel realm, you **learn** from them based on what they tell you about what they know, you **share** the information horizontally throughout the agency and beyond, and you continue to **expand** the breath and scope of that foundation. How do you expand it? See next paragraph.



B. Partnerships

You expand the breath of your intelligence program by creating and leveraging partnerships. Your officers are out there in the field everyday, and inevitably are working with another agency or department. They are the ones capable of sharing information with those partners, and getting information from them. Now in the org chart, this is also where a supervisor in the intelligence realm focuses his or her effort. In fact, it should be their primary focus: building, fortifying and expanding those partnerships. When a real life situation occurs, there has to be a "go to" person within your agency that every other agency has on their speed dial.

C. Connecting the Dots

As the information begins to flow, someone has to take it and digest it. Someone has to link that information to the information from other sources: other officers, databases, research tools, and other agencies.

D. A Product … and Feedback

Ok, so we got the information, we sent it somewhere, someone did the analysis and connected some potential dots… now what? You need to push out the assessment of the data to the leadership that can or will take action. It is your product. If it indicates something that could happen tomorrow, you push out the assessment to the tactical commanders (hence the name "tactical intelligence.) If is predicting a trend or something that could be happening or increasing activity in the future, you push it out to the command leadership that may need to think about reallocating resources or focusing effort in one particular direction. You've allowed the organization to become "strategic" in its actions.

Don't forget the most important product of your assessment; the feedback to the officer that provided it to you. Remember this critical element as it represents the only insurance that your program will continue, will grow, and get better.

Guess what we have just done… we have created a *Process* that takes *Information* and *Analyzes* it in order to create a *Product*. Does that sound familiar? Like the definition of intelligence in the second section of this paper? These are the Fusion Solutions at the top of the pyramid. The key part of the story is that no one element will function independently and be successful. They all have to work in concert, in a *unity of effort* in order to create an Intelligence *System*..

Notice that I have not talked about technology. Although tools are necessary and the better the tool the better the product, the silver bullet doesn't lie in the software. Each one of those steps requires a human element. And not just any human; one with knowledge, training, experience, and relationships.

The officer on the street needs to have enough experience to recognize that anomaly, and the training to know how to flow it. The analysis that is done, like I said before, isn't dependent on a machine or a technology, even though that is important. It requires the training, skills and knowledge of a person who recognizes and utilizes deductive reasoning. The sharing of information or of a product is based on relationships; knowing who needs the information and how to get it to them.

If you understand this and concur, follow me a little further. This gets even better, and simpler.

V. Some History

OK, so let's assume you followed the blueprint and created a great system. We built our pyramid and have a great way of getting lots of information flowing upward and downward, backward and forward. Here is a statement that will pop a lot of bubbles: Intelligence based on overwhelming information regarding the adversary isn't the silver bullet. In fact, an abundance of information may actually hinder your action. Let me give a couple of specific examples as we look back in time.

A. In War, Size (or a mountain of information) Doesn't Always Matter

Alexander the Great

In 331 BC, in a town called Gaugamela in what is present day Iraq, two vast armies collided and decide the future of the world. The Macedonians, about 50,000 strong were led by a 26 year old king, against the period's largest army on earth from the largest empire on earth, a 250,000 man army led by Darius, the king of Persia.

Although young, Alexander was a veteran commander. He had defeated this Persian army multiple times before, and Darius had drawn a line in the sand. This was going to be the deciding moment in history. He had to crush Alexander and he had to do it

decisively. He assembled all of his troops, all of his weapons, all of his might for the show down.

How had Alexander beaten the Persians multiple times before? Well, first, if you grew up in Macedonia, you learned to fight. It was in your blood and in every part of your being. Second, Alexander had already developed brilliant tactics that had proven unbeatable. The most famous was the Phalanx. 256 men in each unit, standing 16 across by 16 deep. A square of tightly aligned men with 12-18' spears and a shield held close by hanging across their shoulder. The shields would face outward from every man on the outside lines, and overhead for every man on the inside lines. They were a block of armor that moved forward in lock step.

Before the battle, his generals present a plan to Alexander that will strike the Persians at night. They feel, based on the intelligence that they have on the amassed forces 5 times their size, that this will be the one and only way Darius will be defeated. Alexander disagrees, and tells his commanders that they will fight them in the morning so the enemy will see openly how they are defeated.

In the battle, Alexander strikes first at the center of the Persian line, but with a tactic that had never before been attempted. He lines up his troops in the Phalanx positions, but he doesn't send each Phalanx into the Persian army line-up head on. He slants them at about a 45 degree angle. He also personally leads one of his cavalry out in a parallel line for miles. Darius is puzzled and orders his cavalry to follow Alexander. This, combined with the attack on the Persian line at 45 degree angles opens a huge gap, and Alexander does a 180 degree turn and launches his cavalry into the gap.

Darius unleashes one of his most dangerous weapons, chariots with blades mounted forward and on each wheel that stretch out 10-12 feet. Alexander's Phalanx units immediately get into a U shaped formation that the horses naturally head into. Once there, they are trapped and instantly eliminated.

Long story short, Alexander defeats Darius and goes on to lead the Macedonians to conquer much of the middle-east.

Lee vs. Hooker

One of the battles that students study in our military academies throughout the world was waged at Chancellorsville, Virginia, in May 1863. It was between the Army of the Potomac, led by Major General Joseph L. Hooker, and the Army of Northern Virginia, commanded by General Robert E. Lee. With a force approximately half the size of Hooker's, Lee achieves a strategic victory that still puzzles leaders today.

Let me ask you a question: Given the plethora of information that we see today and continue to search for, would Lee have made the same decision and advance on Hooker? Let's examine a little closer.

Hooker had 118,000 – 134,000 men, versus Lee's 60,000. Hooker had a tremendous intel network including hot air balloons that flew over Lee's army to verify and confirm their position. Hooker even had spies that were in the confederate to tell of plans and troop movements. His intelligence network was so vast he was able to move over 70,000 troops to Lee's flank without the enemy even knowing. Hooker was so confident that he would defeat Lee he brought his commanders together the night before battle and declared the eminent victory over shots of whiskey.

But Lee uses intelligence as well, and he adds something else to the equation and the information before him. Through surveillance by Confederate general J.E.B. Stuart's cavalry, Lee ascertains Hooker's strength, and based on that alone, many would consider it a wise move for Robert E. Lee to retreat at this time. He was outnumbered with Federal forces threatening from two different directions. What did he do? He attacked.

The question is why did he attack? Lee wasn't fighting this battle on paper; he was fighting in the moment. He wasn't looking and asking for volumes and volumes of data before he made a decision. In that moment Lee had intuition. He had that "feeling" based

on his training, his education and most of all, his experience. He acted on that intuition rather than wait for the data that today's leaders seem to need before making decisive decisions. He had what Malcolm Gladwell in his National Bestseller "*Blink*" writes about. He had the power of thinking without thinking.

Red Cell vs. Blue Cell

Let's talk about one more instance. In Gladwell's book, he describes Paul Van Riper and his "Big Victory." Paul was a Marine who became legendary in Vietnam. In one place where he was assigned as Commander of Mike Company, the rocket attacks were occurring once or twice every week. In the three months he was there, there was only one. He was described by one of his sergeants as a "gunslinger." He went on to say, "wherever the skipper operated, the enemy was put off by his tactics." Riper lead from the front, and by leading from the front, he captured real time data and information about what the enemy was doing and would do. He was decisive and acted on what he "felt" out there in the field.

Well after his distinguished career, the Pentagon came to him in the spring of 2000 to lead the red cell in a war game exercise they named "Millennium Challenge '02," as a rogue commander who had broken from his government somewhere in the Persian Gulf and was threatening to engulf the entire region in war. This rogue had a strong power base of loyalist and four different terrorist organizations. Riper accepted, and so began another legendary story.

The Pentagon spent $250 million planning, preparing and staging this exercise, the largest and most expensive war game in history. They brought together hundreds of military analysts, specialists and software experts and developed the following;

- The "Operational Net Assessment" tool which broke down the enemy into a series of military, economic, social and political systems. It then created a matrix showing how all those systems were interrelated and which of those links were most vulnerable.

- The "Effects-Based Operations," which directed them to think unconventionally to destroy an enemy's assets.
- The "Common Relevant Operational Picture (CROP)," which provided a comprehensive, real-time map of the combat situation.
- And an unprecedented amount of information and intelligence from every US government organization.

Their goal was to lift the fog of war with every sensor, computer, and satellite they had in their arsenal. On the day the exercise began, the Blue Force poured ten's of thousands of troops into the Persian country, had a carrier battle group just offshore, and issued an ultimatum to the Red Cell that called for their surrender. Pretty much had him against the ropes, wouldn't you say?

All their technology told them what the rogue commander was likely to do, and what his vulnerabilities were. They knocked out his microwave towers and his fiber optics, forcing him to use cell phones and satellites to communicate and that way they could monitor what he was saying to his troops. They were confident that they had him right where they wanted him.

So how did it work? He didn't think like the Blue Team, he thought like a rogue commander. He didn't communicate on cell phones like Bin Laden's people in Afghanistan did; he began communicating with messengers on bicycles and through encrypted prayers. He didn't bow down to the show of force that the Blue Team laid out; he launched a surprise attack with a fleet of small boats and bombarded them with cruise missiles. He preempted their strategy of preemption.

"… I struck first," He is quoted as saying. "We'd done all the calculations on how many cruise missiles their ships could handle, so we simply launched more than that, from many different directions…. We picked the ones we wanted."

When the surprise attack was over he had sunk sixteen American ships, and if it were a real war, 20,000 American soldiers and sailors would have been killed before they had even fired a single shot.

B. Thinking Outside the Box (Paradigm Shifting)

What Alexander did, what Lee did, and what Riper did was think outside the box, outside the stovepipe or indoctrination of their agency, their country, or their organization. They didn't think like they were trained to think, they thought the way they instinctively knew how to think with training and experience. They each trusted that intuition that told them the way to win was B and not A. Even though all the data that was being shown to them said something different.

Darius looses because he thinks having the greatest army, the greatest tools, and the most weapons would defeat his small challenger. Hooker lost because he let the data and sheer numbers tell him he was going to win. The Blue Team lost because they had spent countless hours, manpower, resources and money on analysis of every possible contingency.

Yet they all missed the truth. Just like on 9/11, and just like on December 7th, 1941.

VI. What's Wrong with Intelligence?

What's wrong is the systems, the processes, and the quest for information. In one sense, and as many have pointed to, we do not have systems that create that pinnacle on the pyramid. We have disparate organizations that collect and analyze, but don't share it with anyone. We have thrown people into the law enforcement field with "intelligence" responsibilities, but we haven't given them the breath of training and a foundation that they can build upon. And worst of all, we collect a whole lot of information from our people, but don't give them any feedback that says "thanks."

At best, we get information overload. Think about that for a minute and tell me that you don't get a host of emails or text messages everyday, with the bulk of them not relating to your world of work or being anything that your are remotely interested in. Or, in another perspective, have you worked in an environment were leaders want more data when you go to them with an idea or a recommendation on actions that should be taken in your specialty? They want more analysis, more estimates, and more comparisons, more proof that what you are proposing is a good decision.

What inevitably happens in those circumstances? We and those leaders get overwhelmed and overtaken by that wave of information, and miss the truth that was right in front of us. In time, that's what happened on September 11th and that's what happened on December 7th.

In the Top Secret findings of the Naval inquiry to the attacks on Pearl Harbor, some of the findings and conclusions, now open source, were the following;

> "3. A full **exchange of information is necessary** to the effective exercise of Joint Command. While there was a considerable exchange of information between various Army and Navy intelligence agencies **there was no organized system to ensure such exchange**."

"22. Neither the Chief of Naval Operations, the Commander in Chief, Pacific Fleet, nor the key members of the latter's staff, **seem to have given serious consideration after 27 November 1941 to the possibility or probability of an air attack on Pearl Harbor or of its possible effect**."

"28. War experience has shown that:

(a) The responsibility for final major decisions must devolve on one person; that is, there must be **"unity of command."**

(b) In planning and executing joint operations, responsible commanders of the different services, who are to act jointly, and the principal members of their staffs, **must be in close physical touch, and not entirely dependent on telephonic, radio, or similar communications. In no other way can a full exchange of information and ideas be assured nor the possibility of misunderstanding be prevented."**

Interesting that 60 years ago, sharing of information, unity of command, and attention to what was in front of you were the key recommendations. One of the outcomes of the attack on Pearl Harbor was the National Security Act of 1947, which reorganized and centralized the intelligence community with the creation of the Central Intelligence Agency. And from 9/11 in the maritime domain, we have created the Department of Homeland Security, the Maritime Transportation Security Act of 2002, the National Security Strategy, the National Strategy for Maritime Security, the Global Maritime Intelligence Integration Plan, the Maritime Operational Threat Response Plan, the Intelligence Reform and Terrorism Prevention Act of 2004, the 9/11 Commission Recommendations Implementation Act of 2007, to name but a few. All good steps in the right direction, but what will prevent the words I quoted in the first section of this paper from being echoed again?

"Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility, but also responsibility so poorly defined or so ambiguously delegated that action gets lost."

VII. The Solution: It's the Knowledge, not the Information

Here is the secret, the silver bullet. The one thing that is a guaranteed technology that can solve many of our intelligence woes is a unique and unbelievable sensor technology. It has a unique capability to rapidly assess a situation, detect an anomaly, process the information and act tactically. I strongly, forcefully, adamantly suggest that you build your intelligence system using these sensors…. Your officers.

The way to build a strong system, a strong pyramid with a wide and solid foundation, is to focus your effort, your time and your money on the training and tools they need. Build that foundation first, and cement it. The other layers on your system will come.

Why do I consider this so important? Because there is no one thing, no technology looking out in the vast domain, no software that can see inside another man's head, no magic ball that will predict the future. There are, however, hundreds, thousands, millions of officers that can exercise experience, knowledge, and domain awareness to detect that anomaly, can make that behavior identification.

We've proven it. It was the deputy in South Carolina that stopped the students from Florida with "fireworks," it was the Customs officer that stopped the Millennium Bomber, it was the rookie that found Eric Rudolf behind a store rummaging through a dumpster.

VIII. In Conclusion

Really break the mold here and think behind the confines of what we know, what our agency thinks or does, what we've been told it is. Work with me for a moment and erase everything in your hard drive to focus on what I am about to say. It's not an intelligence program, it's not an intelligence plan, and it's not an intelligence system. All those

independently will not provide the solution to the problem. In unity of effort and as a collective process, we give ourselves a chance… but that's not all. We need one more secret ingredient to solve the problem. For a moment, forget the program, the plan, and the system. Think outside the box.

Think *Intelligence Forward*

Think of this in the context that Larry Bird (my favorite basketball player) looked at the basketball court during a game. He was an amazing athlete that became famous for the way he passed the ball, mostly without looking. He just knew where his teammate was, and got the ball there before the player got there.

Wayne Gretzky was another phenom. From a TIME magazine article, he said "I skate to where the puck is going to be." He went on to say, "People talk about skating, puck handling and shooting but the whole sport is angles and caroms, forgetting the straight direction the puck is going, calculating where it will be diverted, factoring in all the interruptions."

What Wayne Gretzky described is called "fast-forwarding" (Sashittal & Jassawalla, 2002) or the ability to travel forward in time and predict where, after seemingly infinite combinations of ricochets and caroms, the puck will emerge-the ability to make his way to the precise spot.

Athletes who fast-forward, anticipate where teammates and the competition are going to be. Using this technique provides a competitive advantage and makes other teammates' performances better. Through this fast-forwarding they are able to achieve peak performance, inspire others to greater performance and motivate others through their focus and intensity.

Folks, the answer lies in our ability to think that way. To get to where the puck is going before it gets there. To see the court in its entirety and know where our teammates are going to be, before they get there. To see the bad thing happening before it happens.

How do we develop that? We invest in our people. We strengthen our knowledge and experience in our respective areas of responsibility by insuring the tools are in the hands of our sensors out on the streets, on the water, or in the woods. We focus on building our system, or process, from the bottom up.

Why is this way the best way, the only way, in my opinion? It was a police officer responding to a fire scene and his flowing of information that led to the arrest of the terrorist bomber Ramzi Yousef. It was Customs Officer Diana Dean who's interview and detection of an anomaly with Ahmed Ressam that led to his arrest *before* he became the Millenium Bomber. It was a North Carolina officer who encountered Eric Rudolf and stopped him from becoming more famous for more bombings with secondary devices that target first responders.

In my world, and in my words, "It's not about knowing what the bad guy is going to do, it's about getting to where he's going before he knows." The only people capable of doing that are our officers… our sensors.