October 7, 2011

Statement for the Senate Committee on Homeland Security and Governmental Affairs hearing on October 12, 2011, 10:30 AM

John McLaughlin

Distinguished Practitioner in Residence
Paul H. Nitze School of Advanced International Studies
Johns Hopkins University
1619 Massachusetts Avenue, NW
Washington, DC 20036
202-587-3224/703-554-5656 ©
202-663-5769 fax

Thanks for asking me to join you today as you delve into this most important subject.

The requirement to share information and the challenges associated with this have been around since time immemorial – and most pointedly perhaps in the profession of intelligence.

Ancient writers such as the Chinese strategist Sun Tzu capture the essential dilemma in stressing both the need to know everything about your adversary and the need to protect what you know from compromise. But Sun Tzu did not have to struggle, as we do, with the global information net, highly sophisticated encryption, complex legal norms designed to protect privacy, and the massive volume generated by things like a ceaselessly expanding internet, SIGINT agencies that, at least in theory, can collect the equivalent of the Library of Congress in three hours, and electronic media that, when found on the battlefield, may contain the equivalent of a small public

library.   If I can use a metaphor I hate, Sun Tsu had many fewer dots to find, much less connect.

In the end, information sharing is not sharing for sharing's sake. It is sharing to increase the chance of discovering things that may be in the data. So our problem is less a matter of collecting information than it is a matter of discovering what's in it – essentially finding the "bad guys" or the worrisome trends.

If there is a key point here it is probably this: Despite the always critical importance of individual intuition, drive, and performance, we are long past the point when we could rely on single individuals or a single human brain alone to absorb, remember and correlate everything required to ferret out people with ill-intent or developments that portend trouble.

In today's world, success in that requires an unprecedented level of cooperation among people with varied expertise, supported by information systems that make that easier, and legal systems and procedures that take all of this complexity into account.

In formulating my thoughts on this, I am drawing on two things: my own experience in counterterrorism in the first four years after 9/11 and, more recently, the study that I and three other panel members completed for the DNI in 2010, focused on the 2009 attempted Christmas bombing and the Ft. Hood shootings.

So I'd like to cover two things in the next few minutes: First, some positive and negative trends affecting information sharing; second, some suggested ways to move forward.

So, let me begin with three positive trends:

First, I think the desire and willingness to share information have increased dramatically since 9/11. It was never as bad before 9/11 as critics imagined, but we are clearly in a different place today. There are still parochial pockets of people who

don't understand the benefits, but the momentum is clearly in the other direction.

Let me be clear, I don't think of sharing as a kind of "nice to have" – that is, we don't need to share just out decency and fraternity. The need arises because different perspectives, different data streams, and varied expertise are necessary to figure things out.

Second, capabilities for sharing have improved, but mostly within agencies. Every major agency has one or several showcase programs that make data access and analysis markedly easier and more effective than even five years ago. Some of these programs are world class impressive. A problem is that most of these programs are within individual agencies and, especially for raw reporting databases, do not operate very effectively across agency lines. A noteworthy exception is the sharing that takes place within the confines of the National Counterterrorism Center (NCTC), which brings together in one place databases from many different agencies.

Third, there is an improved policy foundation for access to and sharing of data. I refer mainly to Intelligence Community Directive (ICD) 501 that contains the essential tools – admittedly hard to implement – that should allow those seeking answers to discover what relevant data exists, request access to it, and have that request professionally and fairly adjudicated.

Those in the Director of National Intelligence Office charged with implementing ICD 501 have a detailed plan that has now moved successfully through the first two phases and has at least two phases to go. Progress is slow but steady.

But there are at least three countervailing or negative trends:

First, the volume of data keeps going up – with no end in sight – ensuring in the process that those who would do us harm can

often go unnoticed without even trying that hard. This flows largely from the fact that we are in the midst of a technological revolution unrivaled by anything in history other than perhaps the invention of the wheel.

In 1952, the year the National Security Agency was created, there were about 5000 computers in the world. Today we have an internet population in the billions surfing through sites that number in the hundreds of billions. Computing power in the world doubles at least every 18 months, largely due to the ongoing miniaturization of electronic circuitry; in 1982, the average microchip had 29 thousand transistors – today it has about a billion. All of this gives the adversary more tools and more places to hide; of course it does the same for us.

These days, it is not uncommon for an intelligence analyst to see his or her daily "take" of messages go from hundreds to thousands overnight. So information sharing is not just about ensuring that information moves across agency or organizational boundaries; it is also about ensuring that individuals receiving data can actually see, comprehend, and assess what is arriving in their "in-boxes".

Second, the breakdown in security discipline in our own government works against sharing of information. Leaks, both unauthorized and authorized, strengthen the impulse to tighten up -- and they reinforce the arguments made by those who stress the risks in sharing and pose obstacles to doing so.

And third, despite the progress represented by ICD 501 -- broader policy, procedure, and law have been slow to keep pace with the challenge. I'll elaborate on this in a minute.

Given this complex picture, what is the way forward? I regret to say that there is no formula for perfection, given that we are dealing with truly revolutionary trends in the production of information.

But that does not mean that we cannot dramatically improve the odds on our side.

To do that, I would emphasize the need for progress on two areas:

First, we need finally to break through the barriers that have for years kept us from bringing the most advanced information technology to bear on the problem. As I said earlier, we have reached the point where we simply cannot count on the human brain alone to do all the work; in fact, I would go so far as to say it is unfair to intelligence, law enforcement, military officers and our diplomats to do so.

The volume is too daunting, the clues too fragmentary, deception techniques too numerous, and the workforce too stretched. Of course, information technology itself cannot solve the problem – but it can prompt humans to look in all the right places, consider pieces of data that might otherwise be missed, and expose relationships that are buried in all the "noise" that this avalanche of data represents.

What stands in the way?

I have not recently had the opportunity to gauge progress, but the last time I checked there were three mega issues standing above all the particular ones down in the weeds.

First, there is in the national security community limited visibility into data that is distributed across multiple separate systems housed in individual agencies;

Second, existing search capabilities do not allow full exploitation of existing data;

And third, there is not a common and widely-shared vision among national security specialists of the end state they want to achieve on information technology and information sharing.

Without such a commonly shared end state, it is hard to make the tough decisions needed to get there.

Going deeper into the weeds on this, there are a number of things that deserve attention in the near term, medium term, and longer term.

To give just one example for each:

In the near term, it important to have more on-line instruction for national security specialists on what data bases exist and what you can expect to find in them.

In the medium term, we should work to improve search capabilities and training in how to use them.

In the longer term and once basic capabilities are improved, we need to introduce more software capable of exposing underlying relationships in large bodies of data – to borrow a phrase from the Markle Foundation's study of this, we need to get to the point where "data talks to data".

If there is one thing that stands in the way of this kind of progress, it is the age old tension between the need to share and the need to protect the information we acquire, especially that gained through intelligence means.

Both sides have valid arguments. Failure to share means that we will not draw on the expertise of everyone able to contribute to solving problems and defending American interests. Failure to protect means that we risk exposing sources, the identity and plans of our officers, and sensitive intelligence methods.

This is merely a technological age manifestation of an ancient intelligence dilemma: the ever present clash between the need, on the one hand, for prudent risk-taking and, on the other hand, the requirements of smart counterintelligence.

Faced with a dilemma like this – really a sort of Gordian Knot in the intelligence profession – leads me ask what management theorists call the "paradigm shift question": What is it that, if we could do it, would revolutionize what we do?

The intelligence officers who figured out how to take photos from space in 1960 were probably answering that question, even though they probably had never heard a buzzword like "paradigm shift".

So what is it that would lead to a breakthrough on information sharing? The closest I can come up with is something easier to say than to do: a common standard for access to data – essentially the virtual equivalent of an intelligence community badge, the innovation that now lets intelligence officers move physically among different agencies.

This would mean for example that an NSA officer would be able to log on through the same portal, or home page if you will, as everyone else in the community to access, let's say, CIA or FBI data, and that CIA and FBI would have confidence that they know who this person is and what they are authorized to access. It would go a long way to giving assurance to those who rightly worry about the counterintelligence threat.

This would need to be backed up by common standards and processes in every agency for data services such as the auditing, processing, storage and retrieval of information.

I don't minimize the difficulty of doing this: it would take decisive leadership, a shared vision, substantial personnel and financial resources, and buy-in from congressional oversight. But unless we do something like this, we'll just keep having the same old argument until the next bad guy gets through the wire.

The second broad problem likely to complicate our efforts, especially the need to identify people inspiring, aiding, or

intending to carry out terrorism, is that so many of them are turning out to be American citizens. The names of al-Aulaqi, Najibullah Zazi, David Headley, Faisal Shazad, and – in the last 24 hours – Manssor Arbabsiar are familiar ones in this room. Others are undoubtedly lurking in the mountains of data we are scooping up daily.

This is a problem with at least three dimensions, and I believe efforts are underway to deal with all of them:

First, I suspect there is still an inconsistent understanding of the laws and regulations that govern the acquisition and sharing of data that touches American citizens;

Second, there is an understandable concern not to violate laws protecting our citizens' privacy. This can inspire a subtle kind of "risk aversion" in dealing with such data.

Third, terrorists in my personal view have figured all of this out. Faisal Shazad, the unsuccessful Times Square bomber, got his US citizenship a year or so before carrying out his act. Such people know that this complicates our task in detecting them.

Finally, looking to the future there is no chance that this is going to get easier. With each incident – the Christmas bomber, the Times Square terrorist, the package bomb plot, the attempt to implant explosives surgically in terrorist operatives – our adversaries seem to be devising strategies that are harder to detect, while systematically exploiting our vulnerabilities.

Information sharing is a huge subject, so I've chosen to focus on what I judge to be the major problems frustrating the unquestioned dedication and hard work of intelligence officers in this most difficult and complex of times. I am very aware, that whatever shortcomings there are on counterterrorism stand out because they are so at odds with the broad pattern of success

our intelligence, law enforcement, and military officers have delivered since 9/11.

As always, intelligence successes are rarely apparent, not only because we cannot talk about them but because they are usually woven invisibly into the fabric of policy successes.

Thank you for the opportunity to testify, and I would be glad to take your questions.