An Interview With William P. Crowell, Deputy Director, NSA

William Nolte

"I believe the partnership between CIA and NSA can work. It requires commitment at the top of the organizations and buy-in at the bottom of both organizations. I don't think that's been achieved yet, but it is absolutely essential to both agencies."

William Nolte works for the National Security Agency.

(b)(3)(c)

William P. Crowell

Editor's Note: Mr. Crowell was interviewed at National Security Agency Headquarters at Fort Meade on 25 August 1995 by William Nolte, a member of the Editorial Board of Studies in Intelligence.

Let's start with some background—how you got into intelligence and your career at NSA.

I was recruited out of college, which makes me like the majority of the professionals at NSA. It was something of a personal thing. I was so intrigued by the test NSA administered, I said to myself, "Any organization that can create a test like that must be an interesting place to work." And so I decided to have the interview. I've never been disappointed, at least not for long. (U)

And you have worked in private industry. ...

I left here and went to a high-tech corporation, working in four areas: imagery (where I got my chance to learn the imagery field); low observables; mathematics research; and command and control systems. I started a business line that broadened their intelligence interests beyond imagery into other areas, including signals intelligence. (U)

But you're not, at least in formal terms, what one would consider a technical person.

No one believes you ever have a life before you come to work at NSA, but I did. I worked for a communications company that had two major lines of work. One was designing and developing commercial communications—radio communications systems and multiuser systems. And the second thing they did was to build listening devices and other equipment for private investigators. In 1957, it was still legal. (U)

I think the thing that is missed about my background is that I used my prior technical experience to my advantage while at NSA. In particular, more than anything, I wanted to do computer work, so in almost every assignment I've had here I was the person bringing in information technology or expanding the use of technology. I've been writing software since the early 1970s in a range of fields, including signals analysis and others, and I've never lost that interest. I still spend 12 or 15 hours every month maintaining my programming skills. (U)

Everyone was so quick to predict that the post-1945 period would be the "atomic age" but missed the coming significance of the computer, which, one

can argue, has proven a far more influential technology.

I had a conversation recently with the head of one of the largest of the computer corporations, and it was not until the 1950s that we began to develop a viable commercial computer industry. They had grudgingly and reluctantly modified some of their equipment so we could do computing at NSA. (U)

Can you identify two or three areas of greatest concern—make-or-break-it issues—as you look to the future of the Community?

Let's center in on information systems and their impact on the two missions of this Agency, protecting US information systems and exploiting foreign information systems. One of the biggest challenges we face is balancing the two, particularly because what we do in the Defense Department and in other areas of the US Government can influence the commercial marketplace. The systems or techniques that we develop have the capacity to come back on us in the form of increasingly sophisticated target systems. So that's one challenge I think is more than a little significant. How to draw a policy to balance those two issues is extremely important to our continued success—on both sides. (U)

The second issue is that information systems are becoming increasingly complex. For example, most communications engineers believe that it's a lot easier to ensure an error-free transmission over modern networks if there is an equal number of 0s and 1s in the communication string. And, therefore, they almost all, after taking lots and lots of channels, and packing them together in time or frequency, and compressing and otherwise manipulating everything in ways that are complex and hard to undo, add randomization in order to get an equal distribution of 0s and 1s. And randomization looks a lot much like encryption, unless you know the way it was randomized. So, it's the complexity of all the different layers of modern information systems—whether it's the information layer, the compression layer, or the signal technology layer, or the randomization layer—that together present a real challenge to the SIGINTer. What you're saying is "undo all of this," and it's exceedingly difficult. (U)

Let me add to all that the third biggest challenge facing us, and that is volume. And I could just end the sentence there and everything is said. But let me just put it in terms that NSA Director Admiral McConnell uses in testimony

(b)(1)
(b)(3)

That gives you some idea of the daunting challenge volume presents, forcing us to look for new technologies. (C)

You don't have to go too far into the public literature to find people saying "volume wins," that the challenge to NSA and its counterparts around the world is going to be overwhelming.

Volume will never win, the reason being that volume is not the only way the world is constructed. The "pipeline" that goes from city x to city y is primarily traffic going between the two cities or going through them en route to some final destination. If you are interested in the communications from th(b)(1) (b)(3) always focus on the pathway between that place and the nearest switch. If you're interested in wireless communications, you can always get close enough to the communications you're interested in that you can "narrow out" a lot of the other volume. And so volume is not the only ingredient; you also have time and space discriminators. Secondly, technologies for dealing with volume are being developed as rapidly as the new information systems are because, guess what, the rest of the world also has to deal with the volume problem. (C)

If you don't believe that, go surfing the Web, with something you absolutely want to find, with no Web Search tools. You'll find out why someone developed Web Search tools. (U)

One can probably find predictions of the impossibility of codebreaking going back into the 1920s.

In the 1950s, when microwave and other point-to-point communications systems were being developed, it was absolutely said that NSA would go out of business. But, as a result of those communications systems, more modern means of collection were invented. When satellite communications came along in the 1960s, we developed ways of sorting through the enormous volumes of communications, dishes on the ground capable of intercepting those

signals, and so on. So, in my view, virtually every communications system that has appeared on the scene, while presenting challenges, at the same time offers extremely exciting possibilities. (U)

Do these challenges require different relationships within the Intelligence Community?

The new information systems do not allow NSA to conduct its mission from a great distance from the target and in a totally passive manner. Therefore, the partnerships we have, let's say first with the military services, because of the need to mix tactical access with national capabilities, must become closer. Secondly, (b)(1) (b)(3) This is absolutely essential. There's no backing away from that, no matter how the supporting (or "nonsupporting") bureaucracies may feel about it. (C)

Do you occasionally feel resistance?

I've spent the last five years trying to tamp down that resistance, with some limited success. But I'm persistent. (U)

But the argument would be, to give it its due, that we have to put extraordinary emphasis on protection of our information, and this of necessity limits how we share and how much we share.

I believe that's an outmoded way of thinking. It's outmoded for several reasons. First, the partnerships I mentioned are essential. You can't succeed without them. And, if you can't find a way to share the information essential to the partnership, then you ought to be prepared to sign up to go out of business. Second, the successes you may be trying to protect, the important sources and methods, have always been and will always be short-lived. You may be able to extend their life somewhat by closing the circle to absolute minimums, but you'll also restrict usefulness. And you'll also restrict the opportunity to be successful the next time, when you're facing one of those inevitable changes. (U)

When you were deputy director for operations [at NSA], you coined the phrase "SIGINT that counts," touching on what you were just saying. To acquire information, process it, and then hold onto it in such a way that it's not useful is not much of a public service, is it?

I have two great fears for the future of the SIGINT system, and I challenge the system as much as I can to react to and mitigate my fears. The first fear is that we will collect what is easy to collect and pretend it satisfies our customers, instead of going after the hard-to-get (politically or technically) information they really need. The second fear is that we'll get the information and then go back to the old days of "tossing it over the transom," as Admiral Studeman used to say, or sending it to the customer and saying "Well, I finished my job. They got it." We need to realize that we have an obligation to make sure that customers get the information, that they understand it, and that they use it. (U)

Pearl Harbor can be described as a cryptanalytic success but a cryptologic failure, in that the ultimatum message was read in time but the information got to the commanders several hours after the attack. That's a terrible but vivid model.

It's absolutely an important message for us to have learned. The other message, one that comes later, and from other wars as well, is that we don't always know what the person at the other end needs. If we rely exclusively on our picks of what to send them, as opposed to relying on their ability to ask us questions or even go through our databases to find what's important to them, we'll probably fail. (U)

Are you comfortable with a system in which the customer judges the success or failure of NSA?

I've always been comfortable with that, as long as the customer is judging success within their area of interest. I don't think we should ask the Commerce Department to judge our ability to support military operations, nor do I think we should ask the military to judge our ability to support economic policy. But, yes, even if we didn't realize it, customers have been making those judgments and affecting our budgets all along. (U)

More so, now?

But more now, particularly since the demise of the Soviet Union. With that event came the drawdown of resources, the shift of priorities, and shifts in thinking about essentiality of intelligence. (U)

Aside from the volume issue, one of the things you must hear—from the academic community, and the press, for example—is that we're experiencing a shift in the value of information. Presidents will be reacting to open-source information, on the Internet or on CNN, and that the relative value of covertly acquired information declines.

I'm not particularly interested, if I may call myself a consumer of intelligence, and I think I am, in things that have already happened. I'm interested in two sets of things: those that will affect my future choices; and those aren't all going to come from open sources. Second, I'm interested in those things that haven't happened yet because they're in planning. I don't think all the important information about critical, developing events are going to appear in the open. (U)

I also think one of the things we try to do too often is to pit one information source or one intelligence source against another, as if it would be possible for us to "pick a winner" and do away with all the other sources. (U)

If you are content to see only the exteriors of buildings and the exteriors of missiles and tanks, then imagery will serve all of your needs, as long as you know where to look. But if you want to know what's inside the building or have some doubt where mobile assets are going to be, you'd better have some robust intelligence sources like SIGINT and HUMINT that can give you that kind of information. So, the truth of the matter is that, even though as a Community we often don't accept this, we need each other. Imagery needs SIGINT and HUMINT to know where to look. (b)(1) (b)(3) There are so many synergies in intelligence sources that we are doing ourselves and our consumers a disservice by "picking the best." I think, in that sense, open source is nothing more than another source of information which you'd better be aware of in order to obtain the maximum efficiency and effectiveness of the intelligence system. But you'd better not put all of your eggs in that basket. (S)

Has the Community been successful in making the case, before Congress, among others, that we have provided information of value commensurate with our costs?

I think that at this moment NSA and the Community in general have strong stock with Congress. But there are areas of weakness we need to shore up. These range from Ames and Guatemala to our ability to cooperate. (U)

DCI Deutch has reaffirmed his support for a policy of openness. How have we been doing with that?

Recently, we've done better. Obviously, the VENONA releases were quite significant, moving in the direction of recognizing when a story can be told. And that's essential. We're not going to become irresponsible. But we are going to become more responsible for being positive in our ability to recognize when stories can be released. What is often forgotten when we talk about protecting sources and methods is why we're charged to do that. Having spent the public's money to develop certain capabilities, the public expects us to maintain those capabilities as viable, as long as we possibly can, and to release those capabilities only when they no longer serve an intelligence purpose. That's an economic issue, but we often turn it into a passionate issue of different proportions. (U)

Not only do we have to change that attitude, because of the recent executive order on declassification, but, and this is a very strongly held personal position, we owe it to the American people to contribute to history what the Intelligence Community has done, once sources and methods are no longer an issue. (U)

VENONA is a classic example of how we can tell the story and convince the public that intelligence, at least historically, had an impact on the direction of the country; on the direction of the world, for that matter. (U)

On VENONA, there was a cost to the United States of retaining that information, in that many Americans grew up believing there was no Soviet spy effort.

As you know, I was involved with VENONA 20 or 25 years ago. It was one story I believed would have to be told one day. It will never end the debate, but now it's in the hands of the historians to make the judgment, not us. (U)

Let's talk about the creation of a National Imagery Agency. What can NSA provide in the way of lessons learned?

Both Admiral McConnell and I have tried to be extremely helpful and balanced in our presentations, discussing the realities of the SIGINT stovepipe as a model for the NIA. (U)

The realities are we don't own everything. And, of course, everyone who wants to reorganize the Community into a new stovepipe wants to own everything, because control makes it a lot easier to get on with things. But the real strength of NSA is technical leadership and technical direction over the many people who

are engaged in SIGINT, including many whose budgets are determined outside the Consolidated Cryptologic Program—(b)(1) (b)(3) I think the imagery problem has to be solved in a similar way. They'll need to decide what the technical issues are and who decides them. What are the resource issues and who will decide those? (S)

Is it fair to ask what pitfalls you've warned about?

There are some large pitfalls, with regard to the relationship between a National Imagery Agency and the organic resources within the military services, the picture-taking aircraft and so on. How do you balance the need for services dependent on those resources with national needs to ensure that there exists interoperability and compatibility between systems? That will be a very tricky area, as it has been for SIGINT for a long time. Not yet solved! (C)

The second area we've cautioned them about is when does an image become "intelligence," as opposed to "imagery intelligence?" How do you judge when someone is doing imagery intelligence as opposed to all-source analysis? We know how tricky that one is. (U)

That raises the question of the stovepipes and the bridges across them.

The term stovepipe is unfortunate. What we are talking about is various sets of professional and technical expertise. And we're talking about building a system of systems, one of which is a SIGINT system that has all of the necessary ingredients of training and development and science that has to do with SIGINT. It's obviously best to put all of that into one organization where it can be nurtured. The same is true of imagery and of HUMINT. You don't want signals intelligence officers out walking the streets collecting human intelligence. They don't have the training or the background. (U)

Where do you build the bridges of cooperation and teamwork? My view is at every level across the stovepipes, instead of trying to build them on top of the organizations. You look for teaming opportunities, whether in the collection arena or in the analytic arena. We need to share technology, we need to share information, and we need to share policies. (U)

You want to encourage people to develop their strengths in a given field, but not to act in ignorance of other fields, correct?

Exactly. That's why the bridges have to be built at virtually every level across the stovepipes. You can't just build them on top. You can't have the DDI at CIA and the equivalents at NSA and DIA as the places where the bridges are built, because what you get is three stovepipes with a plank on top. (U)

When you look to the future and the need for technical leadership, what are your concerns?

My greatest concern is that our current state of downsizing is such we have not had the ability to do any hiring. We will hire 89 people this year. The most we project for the near future is 100 to 200 each year. That is irresponsible but unavoidable under our current authorities. (C)

Based on current projections, that will not turn around for the next five years. And we have not been hiring large numbers for the last four years. So, it could be as long as a nine-year hiatus with only about 1,200-1,500 people having come on board during that entire decade. (C)

At what point does this become damaging?

It's already beginning to have negative effects. Obviously, people coming in from colleges and universities, while not able to tackle our hardest problems, are more up to date on the latest technologies and are able to bring whole new ways of looking at things to our problems. (U)

Back to the main question. Neither NSA nor CIA will ever get people out of colleges and universities—or business, for that matter—that are sufficiently trained or seasoned in this business. We'll always have to invest in specialized training and development. In that regard, I think NSA's strength is our professionalization system, which codifies that training in identifiable directions.

As you look at problems you've dealt with over the last four or five years, how pleased are you with the progress made in transition?

That depends on where you sit. Some people outside the intelligence business may feel we've accomplished a lot, with few tools and little flexibility in making resource decisions. I'm personally disappointed at how long it's taking. Most people within the agency are stunned by

how quickly this is occurring and would like to see parts of the process slow down. (U)

Why am I disappointed in the pace? We are drawing down, we have ever fewer resources. It is no longer possible to push decisions off into the future without it costing a great deal in the way of a continuing resource burden. If you keep open a site that is producing but which you know is no longer part of your future, it can cost, over five years, anywhere from

(b)(1)
(b)(3)

that time. The earlier you make the decision to bank on the future at some present cost, the better off you are. That's what led me as DDO to make decisions resulting in the closure of 17 sites, with the decisions made in less than a year. We've decided to close three or four more since then. (C)

It would not be hard to find critics of those decisions.

(b)(1)
(b)(3)

Any last thoughts?

One of the things I'll throw in is that I had the opportunity to work at CIA in the Directorate of Operations early in my career, and I have spent a great deal of my time in the intervening years working closely with the DO and the Directorate of Science and Technology. As a result of those experiences and based on my analysis of what we face in the future, I believe the partnership between CIA and NSA can work. It requires commitment at the top of the organizations and buy-in at the bottom of both organizations. I don't think that's been achieved yet, but it is absolutely essential to both agencies. (U)

Thank you.

50 USC 3024(i)
18 USC 798
P.L. 86-36