Integrating Intelligence and Acquisition to Meet Evolving Threats

Interview With Dr. Sean Kirkpatrick of the Defense Intelligence Agency

Brian Brodfuehrer

Efforts to improve integration between the requirements community and the acquisition community must now be expanded by adding the intelligence community into that partnership. This is because how we design and employ our systems is heavily influenced by the threats we face. Increased globalization of communication and technology sharing has enabled those threats to become more significant and pervasive, a trend that is not likely to diminish. To stay ahead of that threat, in a cost-effective way, the Acquisition, Intelligence,

Brodfuehrer *is a professor of program management at the Defense Acquisition University at Fort Belvoir, Virginia.* **Dr. Kirkpatrick** *is the Defense Intelligence Officer for Scientific and Technical Intelligence (DIO/S&TI). He is the DIA Director's and Deputy Director's senior advisor on the full scope of S&TI issues spanning analysis, collection, foreign liaison, counterintelligence, strategy and resources across the Defense Intelligence Enterprise.*

and Requirements (AIR) communities must partner in new ways and rely on each other's strengths. This partnership or integration, must be present and active at each level in the Department of Defense (DoD) enterprise—from clear policy and governance down to program management and execution. At a minimum, we need to understand the threat and apply this understanding to drive our research, technology development, technology insertion, and existing program planned product improvements. Likewise, the intelligence community needs increased understanding of the requirements and acquisition demand for intelligence data necessary to build and operate weapon systems that are resilient and adaptable to this rapidly changing threat.

Near the end of last year, I interviewed Dr. Sean Kirkpatrick of the Defense Intelligence Agency (DIA) regarding partnership between the intelligence and acquisition communities. As Senior Scientific and Technical and Intelligence Advisor for the defense intelligence enterprise, Kirkpatrick evaluates what our adversaries are doing and projects what that means to the United States. He is also a level III program manager (PM) and has managed programs at the National Reconnaissance Office, the Air Force Research Laboratory and DIA.

My interview with Dr. Kirkpatrick highlights the importance of building a stronger partnership between the acquisition, requirements and intelligence communities to anticipate and plan for responsive and emerging threats. This partnership must leverage the best of what each community offers to stay ahead of the changing threat.

The following are highlights of that interview in question-and-answer (Q&A) format.

* * *

Q. Why is intelligence support to acquisition becoming a hot topic?

A. The United States is losing its technical advantage through globalization of technology markets, through black markets and through espionage. We are currently coming to a tipping point where our capabilities are in danger of being fielded after the adversary's countermeasures have been developed.

Q. What are key characteristics about the intelligence community that the acquisition community should understand?

A. Unlike physics, intelligence is not an exact science. But, like systems engineering, there is a lot of art and science mixed together. The intelligence community can be thought of as a group of specialists and a group of generalists. The specialists might focus on a type of weapons system or a region in the world or on signals intelligence. The generalists or the "All Source Analysts" bring that all together and provide a complete picture to the policy makers and to PMs. The "All Source Analysis" is more robust and it takes longer to generate. What the acquisition community needs to understand is that the question you ask, the way you ask it, and who you ask it of affect the answer you get. So if you ask the question of a single source analyst, you get a single source answer. And if you ask the question of an "All Source Analyst," you are going to get an all source answer, and it will take longer. Not knowing this sometimes leads to misunderstanding on the acquisition side about why I am getting different answers.

Policy Change on Who Requires Use of Critical Intelligence Parameters (CIPs)

We have drafted policy language that Defense Acquisition, Technology, and Logistics now is coordinating that will make it a requirement for at least Acquisition Category I programs to identify CIPs early and for the intelligence community to monitor those and report breaches throughout the life cycle, especially before major decision points such as Defense Acquisition Boards.

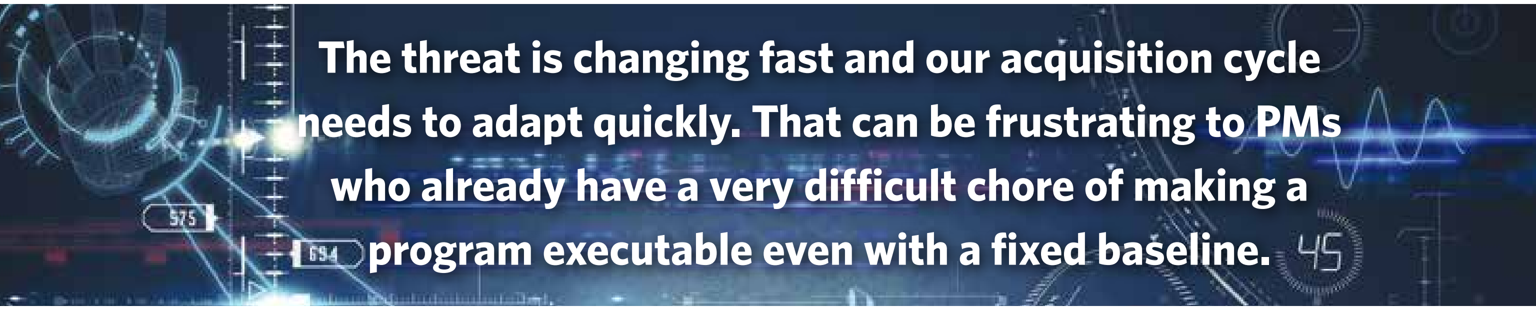
Q. What tensions have you experienced and how would you suggest those be managed?

A. There is a constant tension between the intelligence community and the acquisition community, and it is based on time and certainty. The acquisition and requirements communities want to know what the threat baseline is so they can design their missions or Analysis of Alternatives and then build a capability. They want to know, at a certain time, with certainty, what the threat is. Once they get that answer, they often tell the intelligence community, "Go away, leave us alone and we will see you at the next milestone." What PMs often forget is that it is not about the next milestone; it is about building a capability that will have to win in a rapidly changing threat environment. The threat is changing fast and our acquisition cycle needs to adapt quickly. That can be frustrating to PMs who already have a very difficult chore of making a program executable even with a fixed baseline. The PM must have a constant awareness of what is evolving to avoid the system from becoming irrelevant. And, as we will discuss later, we must adopt more agile acquisition approaches around critical intelligence parameters to account for threat changes.

Q. Where in the life cycle, traditionally, is the intelligence community touching base with the acquisition community?

A. This is something we are trying to change. In previous versions of the DoD Instruction 5000.02, the PMs would get a threat document, they would design to that and they would have to have it updated at their milestone decisions. If the threat changed between the milestone decisions, how likely were the program offices to change any of their system design? They may make note of it and address it in a block upgrade. That, historically, has been an issue. What we are trying to get across in the updated 5000.02 is that the program office should maintain a constant connection with the intelligence community through a liaison officer. That connection would provide updated threat baseline information as part of every major product development decision point; for example, Systems Requirement Review, Preliminary Design Review or Critical Design Review. A goal is to get information from the intelligence community and include that in the list of things that influence design decisions at those key product development points.

In addition, the acquisition community and PMs need to think early on about what information they need from the intelligence community at different product development points. As the design matures, a greater level of threat specificity will be needed. Also, the farther to the left of bang you are looking in the adversaries' kill chains, the harder it is to get intelligence. Being able to write down what is needed and when is important. That is the kind of information that is put in an AISA or Acquisition Intelligence Supportability Agreement. This AISA concept is being piloted right now where the acquisition community identifies what information is needed at each phase of the life cycle, and the intelligence community signs up to provide it. It is kind of a contract between the PM and the intelligence community. In summary, the concept is that there are different levels of intelligence community assessment specificity, and matching the level of specificity to the phase of the life cycle is a way to marry up what the intelligence community produces with what the acquisition community needs.



The threat is changing fast and our acquisition cycle needs to adapt quickly. That can be frustrating to PMs who already have a very difficult chore of making a program executable even with a fixed baseline.

Q. What changes do you see coming in the intelligence community that the acquisition community needs to know about?

A. A number of intelligence support changes are coming. Two important ones are the Critical Intelligence Parameters (CIPs) policy and the change to the System Threat Assessment Report (STAR). Let me start with the STAR: Every system has to have one. Historically, it has been a hard-copy document and has been a snapshot of the threats in a given area of operation. It can range in length from tens to hundreds of pages. If you were to survey the PMs in your next class, I think they would tell you they have been of moderate to low use to them.

Q. Why is STAR of moderate use to PMs?

A. It is a report they have to get, they will read part of it, they are certainly not going to read 600 pages of it, and it goes on the shelf. It usually takes about two years to generate a STAR and get it validated by DIA, and by the time the PM gets it the threat has evolved.

The current process is also inefficient for the intelligence community; it takes two years and a handful of analysts an inordinate amount of time to pull the data together, to analyze it, write it down, get it validated and communicate it out, for many different programs. They are wasting weeks of man-hours documenting all this, which is not doing analysis. We are trying to change the dynamic and pull the intelligence community into the 21st century and get rid of hardbound documents that have limited value. We envision providing an actual multimedia environment that is fully dynamically linked to finished intelligence, to an integrated concept of operations and to threat models. Program offices will be able to grab these intelligence community validated models and use them in their own designs with different levels of fidelity going from early on to test-data-based models. This digital environment is important because analysts then could spend the bulk of their time doing analysis, and the collectors doing collection and not updating hard-copy documents. If a threat changes, the analyst would populate the data base online and update the whole digital dynamic threat baseline, now called the Validated Online Lifecycle Threat or VOLT. The program management office would then get notified if that change is important to them. A PM, government or industry, would much rather get that information when in a flexible trade space than three weeks before the milestone update.

Q. How will PMs know what information they really need to pay attention to? They have a lot of data to cull through. How do they sort the wheat from the chaff?

A. This gets to the second main change. CIPs are vitally important to that. Most PMs don't know what those are. A way to understand a CIP is to think about the adversary developing a capability to neutralize your capability. What key features (parameters) would that system have? Those are the CIPs. What would be its thresholds and objectives? Those would be the particular levels a parameter would need to achieve to be of concern. Those are the things the acquisition community asks the intelligence community to watch and report on. Perhaps a parameter could be detectability. If the adversary can detect a certain level of signal, then that capability becomes an existential threat to your capability and to your mission. The intelligence community needs to let the acquisition community know when that is in danger of happening.

The beauty of CIPs is that the PMs own them. The PM has to identify them early on, and do so in partnership with the intelligence community. It is not everything—just those things that can put your mission at risk. Whatever threat parameter is really important to your ability to conduct your mission and to your capability, we would call a CIP. It is up to the program management office to work with the intelligence community as early as possible to identify those. The acquisition community identifies those early and links them to the VOLT, which flags the intelligence community that these are important and if they change we want to know about it. You can set thresholds and objectives like you do on the acquisition side with Key Performance Parameters. This approach will allow the intelligence community to be more efficient in collection and analysis. Some CIPs will be the same for multiple programs. One threat change could, through the VOLT, flag several programs automatically and when it happens versus one at a time through a hard-copy document around milestone updates.

On the acquisition community side, this has powerful impacts.

The CIPs tell product developers which parameters, if the adversary reaches certain limits, the mission effectiveness of the system will diminish. From a systems engineering perspective, wouldn't I want to design some flexibility around the components that are impacted by these parameters? For example, could I design a modular or upgradable frequency band in a transmission that is supposed to be undetectable?

Another positive thing is that this could reduce the cost of acquisition by not requiring large design margins to account for unknown threat changes. My experience with product design is that, if you don't have a good understanding of where the threat might go, you put in a large design margin to cover yourself. That design margin costs money and can also reduce system performance in other areas. If you knew that you would be watching the threat as the design evolved and that you could upgrade or evolve as required, then you would not have to build in a large design margin early on. This also could avoid expensive technology development to meet a design margin that may or may not be required. The design around the CIP items should be done so that it can be changed in an agile or flexible way, perhaps using a modular open systems architecture approach.

Q. Why do the acquisition community and intelligence community need to be more linked in the future?

A. Fifth-generation weapons systems increasingly rely on intelligence mission data (IMD) to provide their capability. Examples might be overhead intelligence, order of battle information or signatures. PMs need to be aware that if you design the world's most advanced weapon and it requires intelligence mission data to do it, then the intelligence community must be prepared to provide that data. The PM must realize the load that is being placed on the intelligence community and that the requirement for IMD is handing a bill to the intelligence community that may not be currently funded. PMs need to think about what you are counting on from the IC. Do you have an agreement? We must avoid the acquisition community building a system that relies on data that cannot be provided in a timely fashion by the intelligence community. The acquisition community and the intelligence community must increase their collaboration and integration in a much different way to do so. That philosophy extends up the Under Secretary for Acquisition, Technology, and Logistics, Frank Kendall, and he clearly understands that.

The Program Manager and the Intelligence Community: Major Things to Know

- Identify an intelligence liaison officer.
- Request an in-depth briefing on both the threat baseline and on the CIPs for the program.
- Determine if your program is working off a Validated Online Life-cycle Threat (VOLT) or off of a System Threat Assessment Report.
- Get involved with the digital threat assessment pilots.

Q. Is there anything else you would like to add?

A. The only thing I would emphasize is the need for the dialogue, early and often. Have an intelligence liaison integrated with your program management office team. Understand the cultural divide and understand what information needs to be gathered to affect the acquisition program. Right now we are trying to address improvements in the acquisition cycle up to the Milestone Decision Authority. Going into a major milestone, programs will be asked three questions: Have you updated your threat baseline, have the CIPs been breached and have all your intelligence mission data been collected?

The acquisition community and PMs need to understand that there is a cost associated with intelligence. If you are trying to design a system that can defeat an adversary left of bang in the kill chain, then that requires a higher fidelity of intelligence. The farther left you go, the greater the amount of intelligence required to understand vulnerabilities. This costs more. The PMs need to keep that in mind. It gets back to asking, "Am I designing a weapons system that requires intelligence that may be unsupportable?"

There is a need to develop regular dialogue between the acquisition community and intelligence community so that the United States can respond to emerging threats in a cost-effective way. The continued dialogue could reduce cost on both sides.

The author can be contacted at **brian.brodfuehrer@dau.mil**.