Improving Threat Support for DoD Acquisition Programs

Paul Reinhart • Brian Vanyo

Accelerating advancements in threat military capabilities are driving sweeping changes in acquisition intelligence support. Defense acquisition and intelligence leaders recognize that greater consideration of threat capabilities throughout a program’s acquisition life cycle can reduce developmental cost and operational risk. To facilitate threat-informed acquisition decisions, the defense intelligence community overhauled its threat support products and procedures in 2016. This article discusses these reforms and the outlook for improved intelligence integration.

In late 2013, then Assistant Secretary of Defense for Acquisition (ASD(A)) Katrina McFarland formed an integrated product team (IPT) to improve acquisition intelligence support by making it, in her words, “more agile to the emerging threat environment and efficient in the application of better business practices.” Mrs. McFarland sought more rapid delivery of threat information to acquisition customers in order to more effectively support program requirements and design decisions. To that end, she directed intelligence producers and acquisition customers to “work together to develop a better way to make threat support more timely, relevant and dynamic.”

In a series of meetings in early 2014, the IPT studied existing threat support products and practices to develop recommendations for improvement. Initial discussions focused on two intelligence products that have traditionally supported acquisition customers: the

Reinhart and Vanyo are Defense Intelligence Agency intelligence officers who specialize in aviation-related technologies and provide analysis of threats to Major Defense Acquisition Programs. They led many of the integrated product team meetings, working groups, and pilot programs that influenced recent threat support reforms.
Capstone Threat Assessment (CTA), which forecast threat capabilities in specific warfare domains; and the System Threat Assessment Report (STAR), which supported a specific defense acquisition program by identifying all relevant threats and their forecast capabilities at program initial operational capability (IOC) and 10 years after. The IPT identified many problems associated with CTA and STAR development, including the following:

**Insufficient customer support:** CTA and STAR updates occurred biennially with little input from customers on desired content. Regardless, their lengthy production period precluded timely response to any expressed intelligence needs. Moreover, Department of Defense (DoD) policy did not require STAR production to support early program-design decisions that greatly impact program cost.

**Limited threat forecasting:** CTA and STAR threat sections were sometimes more historical than predictive and consequently of limited value to acquisition customers, who often desire 20-year threat projections due to the lengthy span of time between program initiation and IOC.

**Redundant production:** Many CTAs and STARs contained similar threat sections that intelligence analysts had to separately write and review, placing a huge production burden on limited analytic resources in the Department of Defense Intelligence Community (DoDIC).

**Analytic inconsistencies:** Because each CTA and STAR was produced individually on different timelines, they sometimes contained slight differences in analysis.

**Lack of analytic prioritization:** CTA and STAR production is federated among various intelligence support offices, so the DoDIC as an enterprise has little insight into threat topics that affect the most critical or greatest number of defense acquisition programs. As a result, the Defense Intelligence Agency (DIA) could not influence analytic prioritization to better support acquisition needs.

**Proposed Intelligence Reforms**
To correct these threat support problems, the IPT recommended intelligence reforms aimed to reduce production inefficiencies, thereby enabling increased levels of intelligence support throughout a program’s life cycle. The IPT specifically proposed replacing the CTA with a new, centrally managed threat library and replacing STARs with a new product called the Validated Online Lifecycle Threat (VOLT) report.

A VOLT report is the primary threat document supporting a specific defense program. It includes all threat modules deemed relevant to the supported program and explains their relevance to program requirements. The VOLT report also answers specific intelligence questions or requests raised by the program, capability developer, or test representative. VOLT delivery includes a static record copy of threat as well as a dynamic report that is hosted on classified intelligence networks and embeds only the most current threat modules. Therefore, when a single module is updated, all VOLTs using it are updated online simultaneously to guarantee that all affected programs have access to the most current threat information at the same time.

The IPT perceived many benefits of such reform. Centralized management of all threat projections would improve analytic resource management and eliminate redundant and sometimes inconsistent CTA and STAR production efforts. Intelligence support offices traditionally responsible for STAR production would be able to assemble VOLTs much faster and earlier in the acquisition cycle using validated threat content maintained in the Threat Library. Moreover, S&TI experts would have more time to devote to futures analysis in threat module production to improve the overall quality of acquisition intelligence support. Their assignment to produce specific threat modules would also enable more direct feedback from acquisition customers to improve these products. Finally, the dynamic design of VOLT updates would offer programs instantaneous awareness of threat developments to quickly inform acquisition decision making.

Although these proposed reforms were conceptually promising, three pilot programs between June 2014 and March 2015 verified their actual value. VOLT delivery was achieved in a fraction of the time it took to publish a STAR. New VOLT processes drove closer interaction and increased communication between the VOLT author and acquisition customer to improve product relevance. S&TI experts reported spending much less time on threat module production than they typically spent on CTA and STAR reviews in a 2-year timeframe. Finally, the intelligence community demonstrated that dynamic VOLTs could support all programs, even those requiring special DoD clearances.

**Threat Support Reform Implementation**
The pilot programs’ positive findings ultimately led to a formal action for reform. In his April 2015 Better Buying Power 3.0 Implementation Directive, former Under Secretary of Defense for
Acquisition, Technology, and Logistics Frank Kendall ordered the ASD(A) to partner with the Services and the intelligence community to “develop a plan for reducing latency and improving intelligence data integration through transition to the Validated Online Lifecycle Threat (VOLT) and Threat Library.”

Since then, DIA has taken a number of actions to facilitate the expeditious transition to Threat Library and VOLT. It transformed existing CTAs into threat modules to accelerate Threat Library development and to insure against late module delivery by S&TI experts. DIA began tasking S&TI experts to produce threat modules in December 2015 and is validating those modules upon completion. Throughout 2015 and 2016, DIA hosted many working groups of acquisition and intelligence professionals to refine threat module and VOLT content and process requirements. These meetings shaped recent changes to policies governing threat support (DIA Instruction 5000.002, updated on Sept. 19, 2016, and DoD Instruction 5000.02, updated on Jan. 26, 2017) to officially replace STARS and CTAs with VOLTS and the Threat Library. Finally, in late 2016 DIA began developing the Threat Library System, which will host all published threat modules and VOLTS on classified intelligence networks, assist in dynamic module and VOLT production, and enable improved customer feedback; expected completion is late 2017.

Until the Threat Library System is completed, DIA is managing the Threat Library on classified collaborative editing websites. By the end of 2016, the library included more than 100 expert-published threat modules, and almost 200 new threat modules will be published in 2017. For topics that lack a published threat module, DIA has identified approved alternate sources for use in VOLTS.

In January 2017, Service intelligence offices began producing VOLTS in place of STARS, and their anticipated benefits are being realized. VOLT authors have provided threat support within 90 days, and in some cases within 30 days, to sufficiently meet acquisition event timelines. The threat content in published VOLTS is more current than traditional STAR content—by more than 1 year on average. And because a VOLT’s relevant threat modules are continually updated, acquisition customers no longer have to wait 2 years or more (the average STAR-update rate) before being notified of threat developments.

Customer-Driven Production
The biggest change with new threat support procedures is that acquisition customers truly drive VOLT production. DoD policy now mandates VOLT support at the Materiel Development Decision, Milestone A Decision Review, Development Request for Proposals Release Decision Point, Milestone C Decision Review, and the Full-Rate Production or Full Deployment Decision. But acquisition customers may request VOLT delivery to support other events or design decisions as needed.

Customers initiate VOLT production by submitting a VOLT request form and system documentation to their intelligence support offices. In that request, customers communicate key threat areas of interest, select desired levels of content tailoring and provide specific intelligence questions for the VOLT author to answer.

Customers have another opportunity to shape VOLT content at a threat steering group (TSG) meeting, which is a formal threat discussion involving the program manager and/or representative, capability developer, service test representative, VOLT author, VOLT validator, and, as applicable, a representative of the Director of Operational Test and Evaluation. This meeting gives every TSG member the opportunity to comment on the scope of threat discussed in the VOLT and to make other intelligence requests to ensure that the final product best serves each member’s needs.

Threat Support Reform Outlook
When the Threat Library System becomes operational later this year, acquisition customers will have a single place to access all threat modules and VOLTS. They will be able to subscribe to specific threat modules or VOLTS to receive notifications when these products are updated. Users will also have the means to provide direct feedback to module or VOLT authors and drive changes to subsequent product updates.

Feedback is vital to the success of this effort, for it remains a work in progress. A working group of Threat Library System users will continue to shape its requirements during development. The complete list of threat modules will continue to evolve as new modules are added or existing topics are reorganized. Acquisition, requirements and test representatives can help refine threat module and VOLT content by engaging with authors and the DIA.

As these threat support reforms mature, their benefits will likely accrue. The pilot programs already demonstrated that reforms will save the DoDIC thousands of hours of analytic work each year and give DIA leaders unprecedented insight into threats affecting defense programs, enabling improved analytic prioritization and intelligence enterprise management. More importantly, these reforms will enable more responsive threat support to better serve the informational needs of a variety of acquisition customers throughout a program’s life cycle.

In today’s rapidly changing threat landscape, it is vital to our national security that adversary capabilities are considered in every decision that shapes future U.S. defense capabilities. Improved intelligence integration will give acquisition leaders the kind of agility they seek to factor threat developments into milestone decisions alongside traditional programmatic considerations such as cost, schedule and performance. Ultimately, these reforms will arm DoD leadership with the best intelligence today in their efforts to equip our forces for the emerging threats of tomorrow.

The authors can be contacted at paul.reinhart@dodiis.mil and brian.vanyo@dodiis.mil.