The ITEA Journal of Test and Evaluation 2020; 41: 229-232

Mission-Based Risk Assessment Process for Cyber (MRAP-C)

Colonel Martha Monroe
Hanscom Air Force Base, MA

Jeff Olinger
Air Force Operational Test and Evaluation Center, Kirtland Air Force Base, NM

Mission-based Risk Assessment Process for Cyber, or MRAP-C, is an integrated and iterative process designed to benefit a program over the entire acquisition life cycle. The earlier in the life cycle an assessment is accomplished, the better that assessment can influence system requirements and early design decisions. At program outset, the process gives stakeholders valuable recommendations to influence requirements, design, risk management, and test strategy. Throughout the life cycle of a program, the process further informs system development, risk management, programmatic decisions, and test through actionable summaries of system-specific vulnerability exploitation in the form of vignettes.


Colonel Martha Monroe


Jeff Olinger

In 2017, the Institute for Defense Analysis (IDA) published a comparison report on 20 various cyber risk assessment processes across the Department of Defense (DoD) in an attempt to inform program managers on which risk assessment process would be the best to execute, based on the program. While this report was certainly informative and proved valuable to program managers and cyber test and evaluation, numerous processes continued to strain resources. In January 2019, at the request of Colonel Martha Monroe and Jeff Olinger, Major Gen Michael Brewer, the former Air Force Operational Test and Evaluation Center (AFOTEC) Commander, convened a meeting with numerous Air Force organizations to discuss how they may combine efforts and work together to create one methodology to meet all customer's needs. He stated, "Cyber is one of the largest threats to Air Force Weapons systems today." In response, Colonel Monroe volunteered to lead a group of representatives to develop such a process, and formed the Cyber Analysis and Test Working Group (CATWG) to determine a framework methodology for an integrated and iterative Mission-Based Cyber Risk Assessment (MBCRA).

The CATWG consists of 56 members from 29 organizations across the Air Force, and is championed by AFOTEC's Technical Director, Jeff Olinger, to ensure they met the expectations of the AFOTEC Commander. Colonel Monroe facilitated the team and instituted a detailed Supplier, Input, Process, Output, and Customer analysis of each MBCRA. Through this analysis, the teams quickly discovered that many of the steps within their processes were the same. They also learned that the data and input they needed was often the same, as were the outcome and objectives they were trying to achieve. In turn, many of them had the same customers with similar expectations regarding the analysis and report data they needed. Once the team members saw the similarities, they began working to create a "best-of-breed" approach to a cyber risk assessment. In the end, MRAP-C incorporates proven best practices from the Cyber Table Top (CTT), Cyber Blue Book®, Cyber Test Prioritization Methodology (CTPM), Fighter/ Bomber Method, and engineering practices to provide a combined top-down and bottom-up MBCRA. Additionally, MRAP-C shifted the focus from functional design to a cyber-survivable functional design approach, driving the team to establish a new "Phase 0, Cyber Posture" stage to the preexisting DoD Cyber Test and Evaluation 6-phase process. Phase 0 involves performing an early cyber risk assessment on material solutions for consideration during the Analysis

of Alternatives phase to inform the Material Design Decision. But MRAP-C is much more than a process. Through a lengthy process of refining the multitude of steps across the different processes, the CATWG team decided on the critical process steps. Some very detailed work began by creating all of the documentation that support the process. In total, 15 different products exist to support MRAP-C process execution, including analysis, briefing, meeting agenda, test strategy, attack vignette, and final report templates. These are all easily accessible through the team-generated Air Force Portal Workspace. The process and supporting documentation is very mature because the methodologies it is based on are all very mature themselves. Of course, the team did incorporate process improvements while developing MRAP-C. The process drills down to a tactical level to describe each execution step, and incorporates lessons learned and best practices along the way.

Performing a cyber risk assessment like MRAP-C is critical to ensuring the cyber security of Air Force weapon systems. The Government Accountability Office (GAO) stated in the June 2020 Defense Acquisitions Annual Assessment that "More weapon components can now be attacked using cybersecurity capabilities. Further, networks can be used as a pathway to attack other systems." Unfortunately, their report indicates that the DoD does not often factor cybersecurity into Major Defense Acquisition Programs. DoD guidance dictates that programs establish a cybersecurity strategy early to help manage risks as systems mature, and this is where MRAP-C begins to deliver. Programs should begin executing MRAP-C iterations as early as possible in the life cycle. Executing MRAP-C iterations promotes unity of effort while at the same time eliminating redundancy. MRAP-C's iterative nature means that analysis and reporting occur at various times along the acquisition life cycle, with its four major iteration objectives being Cyber Posture, Design Maturation, Vulnerability Verification, and Sustainment. Through the execution of a detailed Functional Thread Analysis, the system's attack surface is characterized and mapped to missions, system functions, and potential cyber vulnerabilities. Cyber risk ratings and priority levels are determined for potential cyber vulnerabilities, and Attack Path Vignettes are generated to highlight potential mission impacts of vulnerability exploitation in a mission context. Additionally, with the iterative nature of MRAP-C, products are created that can benefit the customer for that given time frame in the acquisition process. The report and other artifacts are immediately available for the next iteration to build upon. This saves subsequent iteration teams in both time and effort, as many of the products align across multiple organizations. From the onset, MRAP-C establishes a data repository for all pertinent documentation used during the evaluation process and ensures it is available for other uses. The process yields a single set of living "truth source" documents that meets the needs of the diverse team and fosters information sharing. To help manage these artifacts, Unclassified, Secret, and Top-Secret SharePoint sites exist for all team members of an assessment to access. These repositories facilitate collaboration and information sharing and provide storage for thousands of artifacts that support the process. Early MRAP-C test cases have already received positive inputs from both Risk Management Framework (RMF) and Intelligence personnel stating MRAP-C products saved their personnel weeks of evaluation time.

MRAP-C provides early risk analysis to inform cyber requirements and design considerations as well as to generate a cyber-evaluation methodology to support test community strategies. It also informs the operational community of potential risks to mission success, and the intelligence community of potential vulnerabilities and suggested watch items. At the heart of the process is the goal to ensure a secure system design. The process employs systematic risk analysis to characterize system failure modes and identify potential cyber vulnerabilities early in the life cycle. It helps shape cyber requirements and system design to increase the cyber-survivability of systems. In turn, it accelerates and informs RMF activities by considering planned risk mitigations and protections, incorporates applicable cybersecurity controls in the design, and ensures the RMF team is apprised of engineering, intelligence, test, operations, maintenance, and potential cyber vulnerability risks when performing risk assessment activities and identifying cyber risk mitigations. Furthermore, programs should see efficiency benefits by using MRAP-C. If executed properly, it will reduce overall workload and program cost, and cause a reduction in program schedule while improving system performance. It can also decrease individual workload through use of a larger pool of contributors working together to build common products that can be used by all stakeholders. Finally, it should help decrease the time to field a system by avoiding costly rework involved when finding these cyber vulnerabilities after a system has fielded.

MRAP-C employs an integrated team effort. There is incredible value in having the weapon system operators available during analysis to understand how they would react to any given situation. Cyber can cause a multitude of effects to the system that will force the operators to question their confidence in the information they are

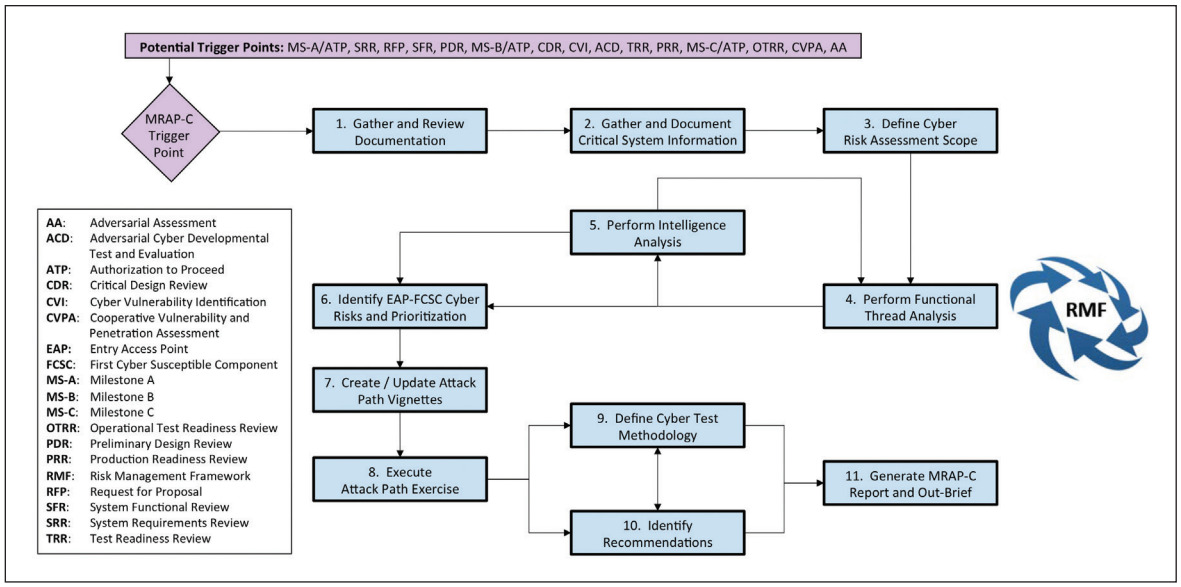
seeing. The ultimate goal is to find vulnerabilities that would cause a mission failure. Maintainers are also included in the evaluation for the same reason. It is important to understand what the common tactics, techniques, and procedures (TTPs) are regarding the system and how cyber vulnerabilities could affect maintenance. For example, if a cyber-vulnerability could cause a maintenance issue that did not allow the jet to leave the ground, then that is a mission failure for the weapon system. The integrated team also includes Mission Defense Team members, intelligence personnel, developmental testers, operational testers, and offensive and defensive cyber testers. Program Office personnel are key to evaluations, as engineers and cyber personnel provide a wealth of expertise. Soon, logistics personnel will join the team to review the supply chain for potential vulnerabilities.

The Air Force Operational Test and Evaluation Center (AFOTEC) and other test agencies transitioned from cyber risk assessments such as Cyber Blue Book® and Cyber Test Prioritization Methodology to MRAP-C. Further, the current AFOTEC Commander, Major General Sears, directed all Acquisition Category (ACAT) I programs to start using MRAP-C immediately. He stated, "MRAP-C is the most revolutionary cyber test process to affect the Air Force in the last decade and we are working with our partners across the acquisition and test communities to implement it as soon as possible." Not only is AFOTEC and the operational testers using MRAP-C, but the 47 Cyberspace Test Squadron (CTS) and the developmental testers are also using MRAP-C on many programs. In fact, Grey Wolf, or MH-139A, used MRAP-C Attack Path Vignettes last year. Other programs, such as Ground Based Strategic Deterrent (GBSD), F-15E Cyber Baseline, and Long Range Stand-off Weapon (LRSO) have adopted the entire process. Moving forward, the plan is to codify MRAP-C into Air Force policy and transition it's ownership over to the Acquisition community early next year. The CATWG is drafting inputs to codify MRAP-C into Air Force policy, making the process mandatory for use by all Air Force Acquisition Programs. In October 2019, the team briefed this concept to Lieutenant General Duke Richardson, Military Deputy, Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics, who approved mandatory Air Force-wide MRAP-C process execution. The first-ever institutionalization of a cyber-risk assessment in Air Force doctrine is revolutionary. It instills the opportunity for program managers to identify risk factors early in system development to avoid impacts to mission effectiveness, greatly enhancing the safety of our people and assets, and ultimately reducing risks to national security. AFOTEC and the various test agencies, like the 47 CTS, will continue to be part of the integrated team, but the acquisition community should employ it early in their programs to get the most benefit out of it. While the Air Force is the primary focus of MRAP-C, the team has received inquiries from other Services as well. They briefed the process at the Cyber Developmental Test Cross-Service Working Group in July 2019 and January 2020 and received a positive response from both the Army and Navy. They plan to present further information to the sister Services and offer training material. They also presented an MRAP-C overview and provided training to Space and Missile Command, who showed high interest in using this process and looking to see how they may incorporate it into the Space Force. The team is also presenting to industry and its associated partners.

MRAP-C is tailorable to fit various programs across air, space, and ground weapon systems, business systems, and both ACAT and non-ACAT programs. It is possible to implement for traditional waterfall acquisition programs as well as Agile and Section 804, and Middle Tier of Acquisition (Rapid Acquisition) programs. MRAP-C is a documented and repeatable cyber analysis and test support process to address all phases of the acquisition life cycle. F-15EX (planned for early next year) is following rapid acquisition process guidelines, as opposed to the traditional acquisition system. Rapid acquisition programs intend to accelerate delivery, and MRAP-C supports this by engaging early to implement an assessment strategy to meet specific timelines.

While there are 11 steps that make up the complete process, the steps do not all have to be executed during each iteration or even executed at the same time. On average, it would take up to about 24 weeks to execute the entire process with subsequent iterations taking less time. MRAP-C began late last year executing various process steps and receiving feedback to make slight changes. The process is now at a point that it is completed and ready to be fully implemented. However, the team feels that there is always room for continuous process improvement. To that end, collecting metrics during MRAP-C events will help to continually strengthen the process and ensure it stays in tune with other initiatives such as Digital Engineering. It is a living process that will continue to be refined as the teams become more knowledgeable on its application and execution.

The MRAP-C process was tested on many programs throughout its development. For example, the team successfully created Attack Path Vignettes for the MH-139 and F-35 Autonomous Logistics Information System (ALIS) programs. The vignettes provide attack objective,



methodology and probable path, potential cyber vulnerabilities, supporting intelligence, and highlight possible mission effects. These vignettes inform follow-on Attack Path Exercise, impact and likelihood analysis, recommendation identification, and the development of specific test methodologies.

To support the integrated acquisition, test, intelligence, support and user community, the MRAP-C Team provides a monthly 4-hour virtual training course. In the first 6 months of implementation, more than 550 personnel from across 25 organizations and all six Services have attended the MRAP-C virtual training. The team also developed a 5-day in-residence course, complete with a detailed case study to facilitate a hands-on experience. This training is in the process of being incorporated into the Defense Acquisition University academia and the Air Force Cyber College studies.

Due to travel restrictions, many of the evaluations scheduled for 2020 shifted right. For the rest of this calendar year, the team is attempting to execute MRAP-C on Ground-Based Strategic Deterrent (GBSD), Long Range Discrimination Radar (LRDR), Long-Range Stand-Off (LRSO) Weapon, and the Advanced Pilot Training (APT) T-7. The team has a robust schedule that shows a timeline of MRAP-C steps to execute based on the cyber-event it is supporting, such as a Cooperative Vulnerability Identification or Cooperative Vulnerability Penetration Assessment.

The guidebook, training, and other MRAP-C products are available on the Air Force Portal at https://www.my.af.mil/gcss-af/USAF/site/MRAP-C. For further questions, you can also contact Jeff Olinger or Colonel Martha Monroe through the Global Email system. ❑

COLONEL MARTHA MONROE is the Individual Mobilization Augmentee (IMA) to the Program Executive Officer, C3I&N Hanscom Air Force Base. She leads the Reserve Team and assists the Program Executive Officer with providing vital support of cyberspace, C2, infrastructure, and cryptologic programs for Air Force, Joint, and Inter-agencies. Colonel Monroe leads and mentors the C3I&N reserve force, and positions resources to provide program support. Colonel Monroe directs military personnel appropriation allocations and utilization. She is also the Lead for the Cyber Evaluation Team, supporting HQ AF Operational Test and Evaluation (AFOTEC). She develops AF strategy for cyber evaluations on air/space/network weapon systems and leads a 52 member Total Force team to perform cyber vulnerability assessments on AF systems.

JEFF OLINGER is the Technical Advisor to the Commander, Air Force Operational Test and Evaluation Center, Kirtland Air Force Base, NM. He advises the Commander and senior staff on the technical adequacy, credibility, and sufficiency of AFOTEC test programs. As the senior technical leader at AFOTEC, Mr. Olinger provides strategic and technical advice to the Commander on test and evaluation issues related to the Center as well as DoD policies, processes, and products.

Mr. Olinger began his government career in 1977 as a graduate of the US Air Force Academy. He completed more than 30 years active-duty service that included time as a command pilot along with tours in Recruiting Service, the AF IG, several tours in operational testing, and as Director of the National Assessment Group. He has an undergraduate degree in Electrical Engineering and a Master's in Systems Engineering from the AF Institute of Technology.