RESEARCH SUMMARY

Wing-Level Mission Assurance for a Cyber-Contested Environment

DON SNYDER, LAUREN A. MAYER, JONATHAN LEE BROSMER, ELIZABETH BODINE-BARON, QUENTIN E. HODGSON, MYRON HURA, JONATHAN FUJIWARA, THOMAS HAMILTON

To access the full report, visit www.rand.org/t/RRA580-1

ISSUE

Wing-level organizations need to assure their mission(s) despite adversary cyber operations. Current initiatives to empower wings to this end are in their infancy. We address ways in which a wing can advance mission assurance in the face of cyber attacks along four strategic lines of effort:

- to defend its systems
- to respond to and recover from cyber incidents
- to maintain resiliency of its missions when systems fail
- to maintain sufficient situational awareness to make decisions to accomplish defense, response and recovery, and resiliency.

In this report, we step through tasks for each of these strategies and identify current deficiencies in each task group along with potential remedies. Not every task for each of these strategies can be done at the wing level. But the wing will play key roles in each. One of the topics we discuss is which roles should be done at the wing level and which should be done elsewhere, supporting the wing.

APPROACH

We conducted a range of interviews to discover the current state of affairs, identify the most important issues to resolve, and elicit ideas for improvement. We also examined the literature on cybersecurity and extracted principles from organizational theory to recommend improvements.

RECOMMENDATIONS

Wing-Level Recommendations

Foremost, we recommend that wing commanders take full ownership of cyber mission assurance of the wing. They must see such resources as Mission Defense Teams (MDTs) as tools at their disposal and use them as needed for the wing's cyber mission assurance. They must also understand that MDTs alone will not provide cyber mission assurance. Every member of the wing and every organizational unit within the wing must play a role.

continued

Therefore, we recommend that wing commanders issue a commander's intent regarding cyber mission assurance of the wing. As part of this command direction, we recommend that wing commanders

- create teams for the ability to survive and operate in a cyber-contested environment who
  - perform and maintain mission maps for the wing using Functional Mission Analysis-Cyber (FMA-C) or a similar method
  - recommend preemptive adjustments to mission architecture for enhanced resiliency
  - devise and exercise plans for mission continuity during and after cyber attacks
  - advise the commander, during and after cyber attacks, of potential courses of action for mission continuity.
- use MDTs exclusively for cyber defense of systems, so that they
  - defend systems, such that some team defends each system type
  - respond to cyber attacks of systems and recover system capabilities thereafter.

We further recommend that wing commanders

- create an appropriate learning culture for cyber mission assurance to solve the many problems in this area that do not have formulaic answers
- develop squadron and group commanders to have better cyber mission assurance expertise so that the next generation of wing commanders possesses better heuristics.

Above-Wing-Level Recommendations

Major Commands and Field Commands

We recommend that Major Commands (MAJCOMs) and Field Commands establish more-centralized command and control for the response to and recovery from cyber incidents, including the following:

- clear thresholds for what constitutes a reportable incident and processes for reporting
- a command center to prioritize response, assign incidents to organizations for triage and assessment, and disseminate and compile findings.

The command center should be

- able to handle command and control for cyber incidents for information technology systems, industrial control systems, and cyber-physical weapon systems
- operational 24 hours per day, able to surge to wartime needs, and able to handle compartmented and special-access information.

We also recommend that MAJCOMs and Field Commands establish accountability for wings and deltas to evaluate wing and delta commanders on their readiness with respect to the commander's intent issued by MAJCOMs and Field Commanders (see the next section). We recommend that this accountability cover

- administrative compliance: Are the directed actions being taken as envisioned?
- operational effectiveness: Are the actions taken by the wing achieving, or likely to achieve, the goal? This component should be included in operational readiness and other inspections to give it the prominence it needs for wing-level readiness.

To facilitate the quality and use of FMA-C products, we recommend that MAJCOMs and Field Commands

- provide quality assurance checks of finished FMA-C products that wings perform
- create training for wing commanders on how they can best use FMA-C products.

continued

We further recommend that MAJCOM and Field Command commanders issue a commander's intent to wing commanders along the lines of directing them

- to defend the wing's critical systems
- to plan and exercise the ability to respond to and recover from cyber incidents
- to plan and exercise means to maintain resiliency of the wing's missions by adaptation when systems fail
- to maintain sufficient situational awareness to make decisions to accomplish defense, response and recovery, and resiliency.

Program Management Offices
We recommend that Program Management Offices

- develop the appropriate tools for cyber defense of cyber-physical weapon systems
- provide technical guidance to MDTs for how cyber defense of cyber-physical weapon systems ought to be performed, perhaps in the form of technical orders
- develop training for MDTs tailored to their cyber-physical weapon system.

Air University
We recommend that Air University

- enrich FMA-C training to help students move from simple classroom examples to the complicated missions of a wing
- provide exemplars or templates of sound FMA-C analysis that are similar to a wing's mission
- expand, temporarily, to provide either reachback capabilities or field teams to assist wings when doing mission mapping.

RAND PROJECT AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. For more information, visit PAF's website at www.rand.org/paf.