Multidomain Protection Operations in a Multicommand Environment

By Lieutenant Colonel Thomas A. Durso (Retired)

and Chief Master Sergeant Christopher C. Nelson (Retired)

The objectives of this article are to demonstrate the friction that we experience in the multidomain/joint protection environment and the challenges that we face in reducing risk when critical assets and/or critical capabilities are not the asset or mission owner's highest priority and to explain how this issue multiplies assumed risk as we move from competition to crisis and into conflict.

Protection in a multidomain, multicommand environment poses challenges for mitigating risk. Most protection professionals understand that criticality is equal to risk, or—

T x V x A$ = R
where:
T = threat
V = vulnerability
R = risk

and that—

R - MR = RR
where:
R = risk
MR = mitigated risk
RR = residual risk

and that, hopefully—

RR x P = AR
where:
RR = residual risk
P = probability
AR = acceptable risk

That seems easy enough. But now, layer the problem set in a multidomain, multicommand environment, where there are blurred lines of equity, responsibility, and ownership, further complicated by the tyranny of distance and multiple plans with multiple phases. Protecting critical assets becomes a science and an art of its own.

As a protection enterprise, we understand that the goal is protecting the capability in order to complete the assigned mission-essential task (MET). Unfortunately, commanders must weigh their METs and apply the principles of war when deciding on the importance of protection—particularly where economy of force, unity of command and, of course, security are concerned. So what happens when a commander is assigned responsibility for protection in the primary domain in another Service command and has little equity in the capability? Compared to the commander's other METs, protection weighs low in priority. If the commander doesn't own the real property or equipment or if the capability doesn't provide a service to the protecting commander, how does the protection enterprise apply protection principles to mitigate the risk?

Insert command authorities and the "art" of protection into the challenge. The ability to apply command authorities to influence the art of protection is, essentially, the ability to thread the seam and close the gap of vulnerabilities. Understanding the complexity of programming, planning, budgeting, and executing ownership across operational control, administrative control, and tactical control lines of authority can help equitably divide responsibilities to achieve a holistic protection capability. In a multidomain, multicommand environment consisting of geographically separated combatant commands, subunified commands, and service component commands, there may arguably be a roadblock that requires a "joint solution to a joint problem." In a fiscally constrained environment, truthful, no-holds-barred assessments and inspections are imperative in order for commanders to understand the assumption of risk and to determine where to apply resources. At many of these crossroads,

where an inter-Service support agreement is not amicable, command-assigned protection is reliant on the joint command to either cut an order or champion the solution. All of this occurs in the critical competition phase of warfighting.

Now that we have explored the challenges of protecting critical infrastructure and ensuring the availability of the capabilities necessary to achieve our METs in competition, how do we achieve the necessary protection effects? These effects must mitigate threats from all domains as we move into the crisis and conflict phases and only have command and control (C2) of primarily land-based capabilities. One of the most basic and enduring fundamentals of joint security operations planning is the establishment of clear, joint security-related C2 relationships. Joint security operations require assigning a single responsibility for protecting the joint force. But when an Army force is designated as the Joint Forces Land Component Command (JFLCC) and assigned as the joint security coordinator in a theater consisting of 90 percent water and hundreds of isolated land masses, this responsibility becomes an exercise in a "coalition of the willing." Coordinating and synchronizing multidomain, joint/combined protection operations in what is predominantly a horizontally aligned, service component-oriented C2 structure is almost a conundrum, with the underlying issue being achieving multidomain effects while not having operational control or tactical control of multidomain forces (save the multidomain task force, which most certainly will not be assigned a security type mission). The most important facets in achieving multidomain effects are possessing operational control of the intelligence, surveillance, and reconnaissance assets; C2 structure; and kinetic/nonkinetic effects necessary to be able to "visualize" the enemy and ourselves (common operating picture) in real time and having the cyber and space superiority to achieve the effects necessary to protect the force.

"We need to take a closer look at the joint concept of protection, what that means to all components, who resources it, and who controls those resources."

As we learned earlier, it is imperative to implement joint risk reduction alternatives in competition; it may be too late when a crisis strikes. If such alternatives are not implemented in crisis, then it will certainly be too late in conflict. Competition is still a rather static operating environment in the land, maritime, and air domains, often (although not ideal) "allowing" single-Service solutions to risk mitigation challenges. But as we move into crisis and potential conflict, the operating environment becomes much more dynamic and money becomes less of an obstacle to achieving joint protection effects than do command relationships; commanders' mission sets; and access, basing, and overflight allowances made by partner nations in theater. Access, basing, and overflight authorities from partner nations are not guaranteed. There is no organizational structure in the Pacific area of responsibility, and partners and adversaries alike vie for regional credibility and partnerships.

So how does the commander of the Theater Joint Force Land Component execute joint/combined protection responsibilities when appointed as the joint security coordinator but does not have operational control of joint multidomain capabilities? How does that commander ensure the security of critical air and sea lines of communication; cyber, space, and electromagnetic domains; and integrated air missile defense? Standardizing protection across the joint force would alleviate much of the burden and help synchronize resources and efforts. As previously alluded, each service component approaches protection differently, with the Army having the most robust approach. Prior to departing competition for crisis, we should all come to an agreement on what "right" looks like within our theater. The pain experienced in cross-component staff coordination in exercises is too much for some and subsequently ignored by others. The end result could be inadequate protection provided by a land force in a predominantly maritime/air domain.

We need to take a closer look at the joint concept of protection, what that means to all components, who resources it, and who controls those resources. How do protection planners synchronize the Army Protection Program with the joint protection warfighting function? The Army Protection Program should be considered a part of competition protection planning and preparation activities, as seven of the Army Protection Program nonwarfighting functional elements directly correlate to protection warfighting function primary tasks. In addressing the needs of multidomain protection operations, we may need to consider developing new protection organizations such as joint headquarters protection cells (or joint security offices) that have the ability to analyze the operating environment and enemy/threats and apply that analysis to account for the capabilities required to achieve multidomain protection efforts. Protection operations differ under multi-domain operations in that emphasis must be placed on cross-domain defense in depth by working with mission partners to identify and mitigate vulnerabilities along the seams between domains (air-land-water interfaces) and to gain awareness/improve coordination regarding overlapping domains (information, cyber, and space).

Lieutenant Colonel Durso (Retired) is a strategic planner for the Mission Assurance Branch, G-34 Protection Division, U.S. Army Pacific, Fort Shafter, Hawaii. He holds a bachelor's degree in mechanical engineering from the U.S. Military Academy–West Point, New York, and a master's degree in kinesiology and optimal performance from Indiana University, Bloomington.

Chief Master Sergeant Nelson (Retired) is the risk management program manager for the Mission Assurance Branch, G-34 Protection Division, U.S. Army Pacific. He holds an associate's degree in instructor of technology and military science from the Community College of the Air Force and a bachelor's degree in liberal studies from Excelsior College, Albany, New York.