Optimizing Security Forces Operations

Employing Risk-Based Strategies

Brandon L. Dinkins

A new Security Forces framework will modernize the forces and establish a comprehensive security posture that will in turn alleviate manning shortages and mitigate detrimental mental and physical health factors for Defenders. Key elements to the new framework include changing policy restrictions, reallocating resources, and improving protective standards.

Security Forces (SF) deficiencies negatively impact the Air Force mission and SF members' physical and mental wellbeing. As such, Security Forces need a new security framework that utilizes personnel and resources to build a more modernized and comprehensive security posture, one that alleviates manning shortages and mitigates deleterious effects on individuals' mental and physical health. Currently, no published works address SF's programmatic process and security requirements to show how they influence a sustainable security model. Operational efficiencies can be improved by changing policy restrictions, reallocating resources to more prominent threats, and creating new protective standards. A less manpower-extensive and more comprehensive approach to base security will avoid levying additional burdens on SF members.

Introduction

The US Air Force Security Forces, also known as Defenders, are the service security and police forces that conduct 24/7 operations to protect personnel and critical national defense resources. Defenders, representing the largest career field in the Air Force with more than 38,000 members, provide installation security efforts at home stations and overseas, including in hostile theater locations. As the service's law enforcement body, SF is primarily responsible for securing resources that provide strategic airpower and protect assets vital to US interests worldwide. Defenders' duties are physically and mentally demanding, and members accomplish many tasks, ranging "from writing tickets to investigating on-base incidents to make sure everyone and everything on every base is protected."[1]

Senior Master Sergeant Brandon L. Dinkins, USAF, PhD, is the superintendent, operations and training, 45th Security Forces Squadron, Patrick Space Force Base, Florida.

1. "Enlisted Security Forces," US Air Force (website), accessed December 17, 2022, https://www.airforce.com/.

Air Force missions largely depend on these individuals to protect their vital warfighting capabilities. For decades, Security Forces have applied a consistent security methodology to provide installation security and base defense capabilities. Yet this has led to security deficiencies and has negatively impacted missions and SF members. The Air Force can improve efficiency by reducing SF policy restrictions, reallocating resources to more prominent threats, and creating new protective standards. Security Forces need a new framework to utilize personnel and resources more effectively to build a more modernized and comprehensive security posture.

By and large, the SF foundation is rooted in requirements-driven policies that significantly restrict commanders from adequately utilizing their forces and forming an adaptive security posture. This method significantly limits how decisions can be made at the tactical level, and several areas of mandated regulatory compliance can form unintended installation vulnerabilities to active shooter attacks, unmanned aerial threats, or complex coordinated terrorist attacks. These inefficiencies routinely impact operational readiness and often require SF units to rotate in and out of 12-hour shift schedules. The threat is always evolving. Because Air Force installations vary in size as well as complexity, SF units require independent security posting strategies to leverage their existing manpower constructs more effectively.

Effectively adapting to threats by integrating security systems and trained SF members requires commanders to track crime and threat metrics, prioritize risks, and create comprehensive security plans. Maximizing SF operations involves methods that systemically build installation-specific strategies. These tailored strategies utilize SF members more effectively, apply appropriate levels of protection to critical resources, and create a sustainable security model that does not jeopardize Defenders' mental and physical readiness. Today, many SF members at Air Force installations worldwide have limited operational effectiveness due to redundant security concepts and restrictive security procedures. A new security management approach for SF posting and response can help create a more lethal, educated, effective, and ready force to meet the dangerous threats of today.

Culture Shift

Many policies that drive SF security operations have not changed since the Cold War. In addition, a wide range of requirements drive SF response priorities, and recent SF leaders such as Deputy Director of Security Forces Tim Gerald have pursued positive change for the entire force. Yet a culture-wide shift to address the many limitations of requirements-based security and the constraints in SF capabilities needs to be made in order to ensure effective and efficient security operations.

In his introductory video presentation to Defenders, Director of Security Forces Brigadier General Thomas Sherman emphasized the importance of a culture of change in today's force, addressing the current global environment, peer competition, and the ability of Security Forces to operate in various settings.[2] Sherman describes how culture

2. Tom Sherman, "Brig Gen Sherman's Message to Defender Nation," Defender Nation, March 10, 2023, YouTube video, 10:20, https://www.youtube.com/.

can shape the path of SF in determining what is needed for airbase defense. Highlighting the need to use technology, equipment, and innovation to transform the Security Forces into a system of record to manage the current battlespace, Sherman notes that Defenders must build the appropriate resources and acquisitions processes to sustain operations. Sherman acknowledges the use of innovation is imperative to shape future operations and create a more agile and comprehensive security posture.

The Problem with Integrated Defense

Procedural installation security guidance is defined primarily in Department of the Air Force Instruction (DAFI) 31-101, *Integrated Defense*.[3] The pacing threat and advancement of technological modernization involve ongoing efforts to improve security requirements and procedures. DAFI 31-101 provides a conceptual framework for the baseline standards of security implementation and defense strategies. Integrated defense is the governing policy that primarily directs how Security Forces implement specific security procedures on installations. It addresses establishing security for protection-level resources, installation access control requirements, and electronic security system implementations.

Yet these requirements often do not account for individual situations at installations; instead they represent a holistic application of security at a foundational level. Many units have unique mission sets with different geographic considerations, which creates challenges for SF commanders—often interchangeably known as defense force commanders (DFC)—to implement strategies unique to their missions. Deviations from integrated defense policies usually require higher-level waiver authority. The SF climate is not accustomed or conditioned to seeking those waivers, especially when it deals with securing protection-level resources. Therefore, higher-level policy should allow for more installation-level decisions to be made by DFCs and in coordination with installation commanders. Fostering a culture where DFCs have more influence to make changes at their level, applying a preponderance of evidence from threat intelligence to create security strategies, can significantly shift SF operations to a more efficient operational climate.

In addition to the challenges posed by a one-size-fits-all security strategy approach, innovation within the SF career field lags behind that of modern aviation and cyber systems across the rest of the Air Force. The Security Forces' innovation and advancement cycle is limited to yesterday's institutionalized standards and compartmented strategies. Defenders use an abundance of manpower to secure resources, critical assets, and airfields rather than integrate technology that augments or even replaces the need for manned security operations. DAFI 31-101 restricts commanders' ability to adapt security standards away from the prescribed requirements. The security convergence of technology and airbase defense can utilize systems to control installation access, surveil and monitor sensitive areas, and deter adversaries. Former Chief of Staff of the Air Force General Charles Q. Brown Jr. stated the Air Force will not grow

3. Department of the Air Force (DAF), *Integrated Defense*, DAF Instruction (DAFI) 31-101 (Washington, DC: DAF, 2020).

bigger in number; instead, the service must adapt to win wars.[4] Air Force Security Forces cannot continue to operate at their current manpower-driven capacity; instead, they must innovate and align with current technology to drive a more robust security posture.

A New Strategy

As within many military organizations, institutional inertia against change tends to persist in Security Forces. Some SF leaders remain steadfast with the status quo and refuse to adopt any new way of thinking. Yet SF leaders have the power to develop a more comprehensive model that reduces manpower requirements while still meeting the appropriate level of base defense and resource protection. Defender units are currently implementing a requirements-based security strategy where their forces are often dedicated to security resources within an inner restrictive area inside an Air Force installation perimeter. Those perimeters contain comprehensive security systems, high-occupancy buildings, structural deterrence, and low threats of hostile actors.

But this strategy requires a security presence that limits other policing activities, creating considerable vulnerability to other installation threats including gate runners, volatile domestic disputes, and active shooters in high-occupancy buildings outside the restricted area. Due to manpower constraints produced by the current security philosophy, as little as one patrol may be responsible for policing areas outside of the priority resources. Conversely, a more suitable strategy would include expanding security efforts across the installation while implementing a priority response matrix for those patrols instead of restricting them to areas with other delay-and-detect systems.

The requirements-based security strategy is the standard security process across the SF enterprise. Gaps in perimeter security have allowed a host of intruders to circumvent procedures at installation access control points. Early 2023 intrusions at Joint Base Andrews, Maryland, have highlighted the limitations in adequately securing Air Force installations, allowing perpetrators to access highly secure areas, even onto aircraft designated for senior US leaders.[5] These security deficiencies can create devastating consequences for high-value assets and disrupt critical mission operations. As one solution, robotic advancements can help strengthen security efforts without increasing the need for manpower.

Technological automation, such as surveillance, can be an effective security solution as it can relieve SF of monotonous and dangerous duties allowing them to provide services in other needed security areas.[6] Defenders at Patrick Space Force Base, Florida, use dog-like

4. Stephen Losey, "Gen. Brown: The Air Force Isn't Getting Bigger; To Win Wars It Must Move Airmen into Undermanned Jobs," *Air Force Times*, August 31, 2020, https://www.airtforcetimes.com/.

5. "Intruder Breaches Base of Air Force One, Shot Fired," CBS News Baltimore, updated February 7, 2023, https://www.cbsnews.com/.

6. Roman Prykhodchenko, Rui P. Rocha, and Micael Couceiro, "People Detection by Mobile Robots Doing Automatic Guard Patrols," in *2020 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, Ponta Delgada, Portugal, April 15–17, 2020, ed. Nuno Lau et al. (New York: Institute of Electronic and Electrical Engineers, Inc., 2020), https://ieeexplore.ieee.org/ .

quadruped unmanned ground vehicles (Q-UGVs) to assist in repetitive tasks like security patrolling around the installation and damage assessments, "saving significant man hours."[7]

This augmentation is an example of integrating technology with new-age security solutions to expand Defender capabilities without increased manning positions. These tools and complementary features are force multipliers and transition away from the static and predictable security model prescribed within DAFI 31-101. Using Q-UGVs is just one of many opportunities to increase security capabilities and reduce the manpower-driven standards correlating to existing SF policy. This strategy aligns with Sherman's intent to capitalize on technological advancement in the career field.

Evaluating Risks

Data consolidation and analysis are a cornerstone for driving informed decision-making. A cognitive approach with an evidence-based strategy can aid in creating a mission-capable security plan. Defense force commanders are mandated by Air Force policy to mass security efforts based on prioritized Air Force resources. Much of the security infrastructure is layered and augmented by a defense-in-depth philosophy where fencing, alarm sensors, and cameras, for example, enhance security integrity. Physical barriers and intrusion detection capabilities significantly enable responding forces to meet hostile actors before they enter protected areas. Yet the lack of innovative security concepts has created many static posts where Defenders are limited in their ability to provide security across different mission areas. A security response team is routinely required to provide inner and outer security for critical- and protection-level resources. But as a result, the team usually cannot provide additional coverage in other installation jurisdictions where a higher threat to personnel is more feasible.

Tracking criminal trends and threats allows DFCs to utilize their force more effectively, thus reducing inefficient policing and security posting. DFCs can reallocate forces to other base patrolling activities and not restrict area security patrols to resources where infrastructure and layered defense can deter and delay adversarial threats. Like the Department of Homeland Security's operations strategy, SF must rely on "timely and actionable intelligence" to evaluate and prevent threats accurately.[8] Directed patrolling, focused deterrence, and joint intelligence fusion can provide a comprehensive security construct that does not require additional manpower to support current posting requirements at SF squadrons around the globe. DFCs should be able to develop a well-defined defense strategy based on current threats and resource priorities.

Such a strategy encompasses more than armed Defenders—hence, the need to use technological detection capabilities and automated systems to augment many posts where complacency

7. Brett Tingley, "US Space Force Test Robot Dogs to Patrol Cape Canaveral," Space.com, last updated August 8, 2022, https://www.space.com/.

8. "Counter Terrorism and Homeland Security Threats," Department of Homeland Security (website), last updated May 30, 2023, https://www.dhs.gov/.

can build over time, especially when coupled with a high operational shift schedule and 12- or more-hour tours of duty. Formalizing an optimal and sustainable shift schedule can significantly reduce risk to installation personnel, resources, and Defenders. As noted by one research study, police officers who worked 12-hour shifts had a lower level of alertness and increased fatigue than those who worked 8–10-hour shifts, thereby creating the possibility of additional security risks and vulnerabilities.[9] Sleep deprivation can have a profound influence on officer safety and survivability by reducing core motor functions and cognitive acuity.[10]

The Risk-Analysis Process

Integrated defense policy significantly focuses on securing installations from external threats and bolstering security for priority resources. Yet increasing evidence shows that prioritizing risk from internal and external threats is a better utilization of forces and a more efficient method of preventing security incidents. Prioritizing risks requires leaders to analyze data and build a security framework that provides critical protection while not significantly detracting from other operational areas. The willingness to assess risk and apply a meticulous security plan for SF must not outweigh the cost of impacting members' overall mental and physical wellbeing. Therefore, commanders should also evaluate the risk to the wellbeing and effectiveness of SF in addition to the risk to resources and personnel.

Policing strategies should routinely adjust to the changing society and incorporate technology within constitutional parameters.[11] By more efficiently focusing security efforts, prioritizing risk ensures the readiness and modernization of base security aspects. Using intellectual energy to enhance the performance of Defenders as opposed to the old manpower-driven security philosophies can increase readiness by providing a more alert, trained force to meet current challenges.

The use of technology in the twenty-first century has changed the dynamic of warfighting and policing. Indeed, the use of technology and real-time monitoring can greatly enhance policing activities and augment SF to reduce specific manning requirements, better prioritizing risk. Unfortunately, Security Forces have had a "do everything" approach and continue to acquire other operational missions without allocating the appropriate resources to utilize capabilities effectively. For example, the use of counter-small unmanned aerial systems is a critical defense asset; however, many SF units are employing this critical capability with organic manpower and may not acquire additional manning billets to employ the system without detracting from other mission areas.

---

9. Karen L. Amendola et al., *Shift Length Experiment: What We Know about 8-, 10-, and 12-Hour Shifts in Policing* (Washington, DC: Police Foundation, 2011), 14, https://www.policinginstitute.org/.

10. Rex M. Scism, "Human Fatigue in 24/7 Operations: Law Enforcement Considerations and Strategies for Improved Performance," *Police Chief Magazine*, accessed December 10, 2022, https://www.policechiefmagazine.org/.

11. Thomas J. Cowper and Michael E. Buerger, "Improving Our View of the World: Police and Augmented Reality Technology," 12, Federal Bureau of Investigation (website), February 2003, https://www.fbi.gov/.

Air Force Defenders have remained a superb fighting force. Nonetheless, their current functionality is not a sustainable model for future base defense strategies. Prioritization creates an accurate assessment methodology to better identify installation vulnerabilities. This can also create more synergy across SF program areas and better integrate security systems into routine operations.

Addressing Security and Policing Limitations

Identifying each aspect of critical systems and assets that require a certain level of protection is paramount to safeguarding them and establishing remedial actions that correspond to each vulnerability. Defenders can use security assessments to identify actions to reduce the risk whenever security gaps occur. Sometimes a collective effort is necessary to close those gaps and provide an analysis process to determine the best solution. A holistic view of program management is important, as well as developing operational compliance standards along the way. Many SF commanders have attempted to implement a modernized method of base security; however, this is not codified across the Air Force. In addition, SF commanders seeking to change the security response efforts must rely on installation commander approval to accept any risk associated with deviation from requirements.

The adaptable capabilities of terrorism have brought a whole new arena of threats, which have forced comprehensive strategies that have interconnections between different geographic locations. Furthermore, not all terrorist traffic and communication are detectable. The more contemporary methods that inspire lone-wolf actors and sympathizers to carry out hostile attacks against soft targets make prevention even more challenging. These threats in the United States and globally have dramatically increased, and of course many terrorist organizations have acted on them.

Military installations have seen more than their share of insider attacks and lone-wolf shooters as well. Notable attacks on military installations have revealed weaknesses in security capabilities and the need for a restructured methodology to prevent hostile internal attacks in addition to external ones. Nidal Hasan's Fort Hood attack in 2009 marked the beginning of "a new adaptation challenge for the Defense Department: rethinking what 'force protection' meant."[12] This attack style further shows the need to preemptively address security limitations rather than wait for a significant event to occur.

The military has encouraged and mandated active-shooter training and preparedness across base populations. This strategy does help to foster a mindset shift in the event of an active-shooter attack. Nevertheless, significant responsibility for stopping an active shooter and saving lives falls into the hands of Defenders. In active-shooter attacks, every second matters, and all too often, manning limitations impact the timeliness of responses. Moreover, the available patrols may be directly allocated to priority resources. Realistically, SF can employ an "all hands on deck" approach to these types of incidents and has, but

12. Amy Zegart, "Insider Threats and Organizational Root Causes: The 2009 Fort Hood Terrorist Attack," *Parameters* 45, no. 2 (Summer 2015): 39, https://press.armywarcollege.edu/.

this is more the exception than the rule.[13] Developing a strategy that allows a more flexible response capability to incidents can generate a rapid response to such high-level incidents. Allowing Defenders to transition beyond their restrictive protection-level post limits expands SF's capability to transition effectively when incidents occur.

Well-developed mitigation plans help build a formidable defense against attack as the evolving environment demands operational efforts exceed the level of existing actual and perceived threats. More resilience in physical security and efficient operations is the ultimate goal; however, enhanced standards have not always translated to foolproof and viable protection methods for those military installations and assets that support national defense. Still, enhanced standards and technology through layered defense allow Defenders to pursue other patrolling activities. Security Forces can utilize patrols as high-visibility deterrence, which helps increase the probability of detecting and deterring criminal acts and security breaches. In addition, such patrolling activity can have secondary beneficial effects by increasing public awareness of the installation and providing additional community enforcement services. This process takes dedicated response teams from static positions and deploys them across a range of security responsibilities, thus increasing their capability to defend the installation and still provide a response to high-priority resources.

Conclusion

Defenders continually answer the call to serve our nation. Their dedication to duty helps instill a feeling of safety throughout the installation and of assurance in the Air Force mission. Providing a comprehensive approach to base defense requires examining appropriate strategies to help build a more effective security and policing framework. Current security posting requirements are deeply rooted in headquarters policy and reduce mission effectiveness at the installation level. Applying an intelligence-driven operational methodology allows Security Forces to transition from reactive strategies to a proactive framework. Refining planning and risk-management strategies against more sophisticated threats is necessary to organize SF manpower and acquire a complementary security system. No single security strategy or detection system will work for every SF unit. Therefore, defense force commanders should identify which methods of security complements and enables their mission without negatively impacting the quality of workforce factors and the individual wellbeing of Defenders.

13. Headquarters, DAF, *Active Shooter*, Air Force Tactics, Techniques, and Procedures 3-4.6 AS (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, February 11, 2018), https://static.e-publishing.af.mil/.