Purple Teaming with Offensive and Defensive Cyber

By CW2 John Mosqueda

The dynamic between offensive and defensive cyber operations is fascinating; though offense is often seen as having the strategic advantage, truly effective security depends on integrating exploitation capabilities with continuous monitoring and incident response capabilities. Depending on their risk appetite, organizations often segregate offensive and defensive cyber teams due to the inherent risks of offensive operations, yet this separation prevents them from gaining the broader perspective that integrating both sides can provide.

The convergence of offensive and defensive cyber operations through Purple Teaming bridges this gap by fostering knowledge sharing of adversary emulation techniques and leveraging established frameworks such as the Cyber Kill Chain and MITRE ATT&CK to evaluate and strengthen defensive postures. This collaborative methodology promotes a proactive security culture that enhances threat detection, accelerates incident response, and reduces the likelihood of network intrusions. Ultimately, the relationship between these two dynamic

Members of various organizations and countries participate in training during exercise Cyber Shield 2025 in Virginia Beach, Virginia, June 3, 2025. In addition to the diverse representation from states and territories, Cyber Shield 2025 includes participants from 38 states, territories, and the District of Columbia along with 15 countries within the National Guard's State Partnership Program. This collaboration fosters knowledge sharing, cross-state cooperation, and a unified approach to defending against cyber threats. (U.S. Army photo by Staff Sgt. Jasmine McCarthy)

ATT&CK Tactic	Technique	Purple Team Activity	Detection Capability
Initial access	Phishing	Simulated phishing campaign	Email filtering and monitoring
Execution	Command scripting	Obfuscated script execution	Script logging and analysis
Persistence	Account creation	Unauthorized account creation	User privilege monitoring
Privilege escalation	Vulnerability exploitation	Exploit execution	Behavioral analysis from user activity
Defense evasion	Clearing tracks	Event-log manipulation	Log forwarding and analysis
Credential access	Password spraying	Authentication attempts	Authentication monitoring
Lateral movement	Remote services	System/account misconfiguration	Network connection monitoring
Exfiltration	Data transfer	Encrypted data transfer	Network-anomaly detection

Table 1: Purple Team Activities Mapped to MITRE ATT&CK Framework (Mettu, 2024)

teams not only validates an organization's security posture but also elevates adversary emulation efforts to more accurately reflect real-world threats.

Evolution of Cyber Operations

With the advent of cyberspace, military operations experienced a significant technological shift through the establishment of the cyber domain. Understanding the evolution of cyber operations is essential to examining the integration of offensive and defensive cyber capabilities. Early cyber activities focused largely on isolated network disruptions, reconnaissance, and attacks against critical infrastructure. As the domain matured, however, cyber warfare became integral to strategic military planning and armed conflict (George, 2021). Cyber operations now shape modern international conflicts and national security strategy, producing implications that extend beyond purely tactical effects. At the same time, the balance between offensive and defensive cyber operations has evolved, demonstrating that neither side holds a decisive advantage; instead, their interaction and integration increasingly determine operational success (Huntley & Shives, 2024).

Building on this evolution, the United States in 2018 adopted the Defend Forward strategy that caused a major shift from a reactive defense to a proactive posture aimed at engaging, disrupting, and halting malicious adversary cyber activity at its source before it can impact U.S. networks (Murphy & Borghard, 2020). This forward-leaning approach strengthens deterrence, enhances security partnerships through "hunt forward" missions, and enables the U.S. to degrade adversary capabilities below the threshold of armed conflict. It also fosters persistent engagement by deepening collaboration with allied partners through coordinated Hunt Forward Operations, during which network defenders jointly identify and neutralize malicious activity within partner networks.

Offense Informs the Defense

The guiding principle of offense informing defense is central to the MITRE ATT&CK framework, which organizes tactics, techniques, and procedures derived from real-world observation of adversary behavior (MITRE Corporation, n.d.). Instead of prescribing a static checklist, MITRE ATT&CK offers a behavior-based model that describes how threat actors conduct offensive operations across each phase of the cyber kill chain. By grounding defensive planning in documented offensive techniques, defenders can better prioritize detection, mitigation, and response actions that directly disrupt adversary tactics. This offense-informed approach enables organizations to assess their security posture, identify gaps, and align the right resources, reinforcing the idea that offensive cyber is a prerequisite for effective and adaptive cyber defense.

Introduction of Purple Team Methodology

The shift from traditional perimeter-based security has driven the development of Purple Teaming, a methodology that integrates offensive and defensive security teams to enable collaborative feedback and shared objectives. Purple Teaming emerges as a collaborative paradigm designed to overcome the limitations of checklist-driven assessments and finalized reports that lack operational context. This integration enables structured adversary emulation, collaborative threat detection, and joint analysis of security controls using the MITRE ATT&CK framework. It also establishes a common operating picture and shared understanding of both offensive and defensive capabilities.

Unity of Effort Between Offensive Cyber and Defensive Cyber

Conventional war-gaming often lacks real-time collaboration with the adversary, given the inherent focus on each side seeking a strategic advantage. Purple Teaming addresses this gap by enabling network defenders to develop a broader perspective of the cyber kill chain while simultaneously refining defensive capabilities to better detect and respond to malicious activity. This collaborative effort between two distinct disciplines is strengthened by applying the MITRE ATT&CK framework, which maps adversary behavior from initial reconnaissance through actions on objective. The framework offers a detailed taxonomy of attack vectors organized by tactical objectives and provides insight into potential adversary motives as a reference model.

Purple Teaming creates a continuous feedback loop in which offensive actions are jointly analyzed with network defenders, accelerating threat detection and incident response capabilities. This process allows defenders to validate their responses against coordinated techniques simulating realistic adversary behavior rather than hypothetical, untested scenarios. Collaboration between offensive teams and network defenders is reinforced by standardized vulnerability-disclosure processes that ensure findings are communicated with sufficient technical and operational context for effective remediation. Over time, these integration practices mature, shifting from occasional joint exercises to sustained operational alignment that incorporates an adversarial perspective into defensive activities while providing clearer insight into the impact of each finding.

Challenges of Siloed Cyber Operations

Cyber Red Teams originated in the military, where they act as opposing forces that emulate enemy tactics to test and strengthen defensive capabilities (Mettu, 2024). In the field of cyber, Red Teams were designed to expose potential vulnerabilities within the organization and perform adversary emulation to gain access to the network. Blue Teams emerged in parallel as specialized defensive teams tasked with implementing security controls, monitoring the network, triaging alerts, and responding to potential incidents. Traditionally, these teams operate in silos with limited interaction due to differing objectives and command structures. This divide has created communication gaps and misunderstandings that hinder the effective translation of vulnerability findings into improvements in the organization's security posture.

Differing perspectives coupled with distinct command structures often foster an entrenched organizational culture resistant to broader viewpoints. Addressing these cultural challenges requires a systematic approach that acknowledges legitimate concerns while demonstrating the value of collaborative knowledge sharing. Awareness of siloed challenges is pivotal, but leadership buy-in is equally crucial for overcoming resistance to collaborative sharing. Collaborative exercises generating shared experiences cultivate trust among traditionally isolated teams, establishing a basis for continuous cooperation. By addressing organizational concerns and risks that contribute to resistance, these initiatives pave the way for a smoother transition to integrated security operations.

Experiences from the Joint Readiness Training Center on Purple Team Effectiveness

Joint-training environments such as the Joint Readiness Training Center (JRTC) demonstrate the effectiveness of integrating offensive and defensive cyber operations through structured collaboration. During large-scale training rotations, Senior Officers, Warrant Officers, and Noncommissioned Officers at the Brigade and Division levels across multiple formations such as the 82nd Airborne Division, 101st Airborne Division, 10th Mountain Division, 11th Airborne Division, 25th Infantry Division, and various National Guard units were coached and mentored on the execution of defensive cyber operations while synchronizing offensive cyber effects with the Army Cyber Red Team. This integrated approach drastically bolstered the organizational security posture by aligning defensive actions with realistic adversary behavior.

Continuous collaboration between the Army Cyber Red Team and the JRTC Operations Group enabled

Table 2: Comparison of Red, Blue, and Purple Team Characteristics (Mettu, 2024)

	Red Team	Blue Team	Purple Team
Primary Focus	Offensive security testing	Network monitoring	Collaborative security improvement
Approach	Simulates adversary techniques	Implements defensive measures	Combines testing with validation
Measures of Success	Exploitation of vulnerabilities	Prevention and detection	Improved security coverage
Timeframe	Limited engagements	Continuous monitoring	Iterative improvement cycles
Knowledge Sharing	Final reports only (may take time)	Internal documentation	Continuous feedback loop

the development of a sustained working partnership focused on emerging cybersecurity trends and recurring operational issues affecting U.S. Army Forces Command (FORSCOM), now United States Army Transformation and Training Command (T2COM). This partnership ensured that training scenarios reflected contemporary threat environments and promoted a shared understanding between offensive and defensive cyber teams. Training conducted alongside the Army Cyber Red Team personnel provided insight into adversary tactics, techniques, and procedures (TTPs), which were subsequently mapped to defensive countermeasures using the MITRE ATT&CK framework. This methodology supported effective attack attribution, enhanced risk assessment, and facilitated the transition from reactive defensive measures to threat-informed defensive operations.

As Divisions assumed greater responsibility as the unit of action, the scope of Purple Team exercises expanded from the Brigade level to the Division level to improve command-level visibility and defensive coordination. This shift, implemented during the 101st Airborne Division Command and Control (C2) Fix rotation, enabled divisions to design, establish, and operationalize Division-level Security Operations Centers (SOCs). These efforts incorporated innovative uses of Security Orchestration, Automation, and Response (SOAR) capabilities to enhance overall defensive posture. In one instance, the 10th Mountain Division established a functional Division-level SOC during an active Red Team engagement, significantly improving continuous network monitoring, incident response capabilities, and validation of threat-detection mechanisms.

The expansion of Purple Team activities also extended beyond the training environment to support forward-deployed operations. In one instance, collaboration between the 82nd Airborne Division and JRTC enabled the development of a continuous monitoring solution while the Division was deployed forward in Romania. This capability allowed network defenders to detect Cyber Red Team activity in near real time, demonstrating how integrated offensive and defensive cyber efforts enhance situational awareness and defensive responsiveness in operational environments rather than exclusively during training exercises.

Recommendations

Sustained Purple Team operations rely on structured, continuous improvement processes that systematically identify, implement, and validate security enhancements derived from exercise findings. These processes should define clear workflows for translating offensive findings into concrete defensive improvements, assign ownership for remediation tasks, and track implementation progress. Periodic reassessment of previously identified vulnerabilities helps verify remediation effectiveness and detect any regressions that require further attention. Feedback mechanisms should capture insights from both offensive and defensive personnel on the effectiveness of collaborative processes, enabling ongoing refinement of Purple Team activities.

Leveraging observations from previous engagements further supports continuous improvement by documenting findings, remediation approaches, and lessons learned, building a knowledge base that informs future security decisions. Regular review of metrics against established baselines helps identify trends on emerging issues that may necessitate strategic adjustments to the Purple Team approach. Incorporating external threat intelligence ensures that Purple Team operations evolve alongside changes in the threat landscape and remain aligned with current adversary techniques. Finally, maturity assessment frameworks such as the Cybersecurity Maturity Model Certification (CMMC) 2.0 offer a structured means of evaluating progress in developing collaborative security capabilities over time, providing input to strategic planning for capability development (Garba, Siraj, and Othman, 2024). Together, these practices create a systematic approach for continuous security improvement that maximizes the value of Purple Team investments while ensuring defensive capabilities keep pace with emerging threats.

Building Adaptive and Resilient Capabilities

Organizations are overwhelmed by vulnerability data and outdated Plans of Action and Milestones (POAMs) that follow a compliance-driven checklist approach. This method fails to manage risk effectively, merely adding

An Air National Guardsman participates in training during exercise Cyber Shield 2025 in Virginia Beach, Virginia, June 3, 2025. The mission of Cyber Shield is to develop, train, and exercise cyber forces in the areas of computer network internal defense measures and cyber incident response. Participants engage in rigorous training courses, including CASP, Pen Test +, CySA, SANS Operational Technology course and more. (U.S. Army photo by Staff Sgt. Jasmine McCarthy)

to organizational workloads without meaningful impact. Without context on how vulnerabilities could affect operations, they become mere noise and contribute to the success of nation-state actors dominating the cyber domain. Organizations must cultivate a cultural shift toward collaboration between offensive and defensive cyber disciplines, asking targeted questions about how specific vulnerabilities could provide avenues of approach for advanced adversaries to disrupt operations.

Threat-informed defense embraces continuous validation through collaborative Purple Teaming exercises. Organizations can leverage offensive cyber capabilities to identify exploitable vulnerabilities within their operational environment, prioritizing remediation for the most critical systems (Sundar, 2025). Threat intelligence enables real-world emulation of specific TTPs used by Advanced Persistent Threats (APTs) targeting critical infrastructure that test the organization's detection and response capabilities. Shifting from a fear-based view of Red Team assessments to a growth-oriented mindset reframes these engagements not as public critiques of competence but as opportunities for self-awareness about organizational readiness. This requires embracing discomfort and redirecting focus toward validating detection and response mechanisms while fostering collaboration with network defenders.

Conclusion

The integration of offensive and defensive cyber operations through Purple Teaming offers a groundbreaking response to near-peer threats in a continuously evolving domain. Bridging traditional silos between offensive teams and network defenders creates a dynamic security model that aligns defensive strategies with real adversary behavior through threat-informed defense. This shift from siloed operations enables near real-time collaborative adversary simulation, where offensive insights instantly validate security mechanisms and strengthen defenses by highlighting the inadequacy of conventional approaches against sophisticated threat actors exploiting control gaps.

Frameworks such as the Cyber Kill Chain and MITRE ATT&CK map adversarial tactics to corresponding defensive countermeasures, enabling more targeted responses. However, sustained success requires comprehensive shared objectives, clear measures of effectiveness across both disciplines, and strategies to overcome organizational resistance to integration. As cyber threats grow more sophisticated, this collaborative methodology builds adaptive, resilient processes to counter determined adversaries in real-world scenarios. Ultimately, embracing dual perspectives enables organizations to move beyond static vulnerability checklists toward cultivating resilient architectures that counter evolving adversary tactics with precision and foresight.

CW2 John Mosqueda is a Cyber Defense Tech serving as a Cyber Planner for the Joint Readiness Training Center (JRTC) and is responsible for integrating Offensive Cyber Effects with the Army Cyber (ARCYBER) Red Team and advising each JRTC rotational unit on implementing internal Defensive Cyber Operations. He holds a Master of Science in Cybersecurity Technology from the University of Maryland Global Campus and has passed the cybersecurity industry's respected Certified Information Security Manager (CISM), the Certified Information Systems Security Professional (CISSP), and the Practical Network Penetration Tester (PNPT) certification exams.

References

Garba, A. A., Siraj, M. M., & Othman, S. H. (2024). An explanatory review on cybersecurity capability maturity models. *Journal of Cyber Security and Technology Studies*, 762–769.

George, N. (2021). Cyber warfare evolution and role in modern conflict. *Journal of Information Warfare*, 20(4), 210–218.

Huntley, W., & Shives, T. (2024). The offense-defense balance in cyberspace. In *Proceedings of the European Conference on Cyber Warfare and Security* (Vol. 23, No. 1, pp. 210–218).

Mettu, B. P. R. (2024). Collaborative cyber defense: A framework for purple team integration in countering sophisticated adversaries. *Journal of Cyber Security and Technology Studies*.

MITRE Corporation. (n.d.). MITRE ATT&CK: A knowledge base of adversary tactics and techniques. Retrieved January 31, 2026, from https://attack.mitre.org.

Murphy, P. J., & Borghard, E. D. (2020). To defend forward, U.S. cyber strategy demands a cohesive vision. The Cyber Defense Review, 5(3), 15–48.

Sundar, S. (2025, April 22). Threat-informed defense is a mindset, not a technique. Center for Threat-Informed Defense (MITRE). https://ctid.mitre.org/blog/2025/04/22/threat-informed-defense-is-a-mindset/.