

The Battlefield is not ‘Over There’ – It is Here, 24/7

Changing Communications for Today and Tomorrow

Lieutenant General Jeth B. Rey

Headquarters, Department of the U.S. Army, Washington, DC, USA

Lieutenant General Jeth Rey is the Deputy Chief of Staff, G-6 of the United States Army. As a principal military advisor to the Chief of Staff of the Army and the Chief Information Officer (CIO), he is responsible for planning, strategy, network architecture, and implementation of Army command, control, computers, and communications (C4) systems. He also oversees cyber operations and networks for Army operations globally. In this ever-present, constantly evolving cyber battleground, the Army is relentlessly pursuing technological advantage by prioritizing capabilities such as the Electronic Warfare Planning and Management Tool (EWPMT), and by conducting realistic, demanding training and wargaming at all echelons and in joint environments. Maintaining the strategic high ground in the contested digital domain—which links Soldiers and battlefield sensors to command centers and weapons systems—requires a team effort. This includes leveraging the combined expertise of Soldiers, scientists, engineers, analysts, operators, and leaders across signal, cyber, and electronic warfare forces. A failure to build resilience, confidence, and trust hinders the accomplishment of the mission. If unprepared, commanders and lives are at risk when adversaries inevitably disrupt and deny access to the tools and spectrum upon which they depend. In a fight against a determined and sophisticated opponent, there is no certainty that these digital capabilities will always be accessible, here and now, in the most decisive moments of battle.

Keywords: electronic warfare, battlefield communications, cyber resilience, non-kinetic dominance, military training, network unification, warfighting

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.*

© This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



Lt. Gen. Jeth B. Rey is the U.S. Army Deputy Chief of Staff, G-6, and serves as the principal military advisor to the Chief of Staff of the Army and the Chief Information Officer for planning, strategy, network architecture, and implementation of command, control, computers, communications (C4) and cyber operations and networks for worldwide Army operations. Since 1983, Lt. Gen. Rey has successfully served as an enlisted Soldier, Warrant Officer, and Officer including assignments in Special Operations units, the Ranger Regiment, and the White House Communications Agency. He has earned Masters' degrees in Telecommunications Management from Webster University, National Security Studies from the U.S. Naval War College, and Strategic Studies from the U.S. Army War College.

INTRODUCTION

For too long, the American military and our citizens have viewed war as happening “over there” in a distant region of the world. But in cyber war, the battlefield is already here in our daily lives – on our phones and smart devices, in our digital infrastructure, across the Electromagnetic Spectrum (EMS), and hovering unseen in our skies and beyond. Ubiquitous technical surveillance, autonomous drone swarms, electronic warfare (EW), and cyberattacks are converging. Our Army must adapt, transform-in-contact, and prepare to deploy for large-scale combat operations (LCSO). To keep pace, we must never lose the initiative.

Data and communications links are the backbone of our Army’s modernization and will be at the forefront of all phases of war in the future. From the homeland to global theaters of operation, conflict in cyberspace is ongoing, 24/7, with adversaries constantly probing our networks and critical infrastructure. Whether on the battlefields of Ukraine or Gaza, where new technologies and all-seeing sensors have transformed the way battles are fought, or elsewhere, war lurks in the shadows and the invisible battlespace of the cyber domain, the EMS, and the orbits of space. When the line is crossed and our Army is called upon to fight, will we be prepared to conduct LCSO an ocean away? I believe we will, but that will require immediate action across several areas.

My unswerving focus is on enabling our Army’s ability to fight and win. Operationally, resilient connectivity of our deployed land force with the rest of the Joint Force is an imperative. Restrictive silos must be proactively eliminated, and our EW, cyber, and network operations must be built into cohesive, innovative, and integrated parts of our formations. Collaboration is essential for us to fully understand the operational environment, visualize and maneuver in the spectrum, and effectively bring all our capabilities to bear against our enemies. Tactically, we must train in realistic environments where navigation and spectrum are denied or congested, against opposing forces (OPFOR) that are empowered with sensors, cyber, and EW capabilities which accurately emulate adversaries. Strategically,

as we embrace new technologies in all our battlefield systems and evolve our networks to handle the volumes of data our Army will use to deploy and conduct LSCO, enabling resilience should these capabilities fail or be attacked is key. And cyber policies must evolve to enable and empower combatant commands and clarify authorities in the Mission Partner Environment (MPE).

With an initial focus on winning the war already upon us, 24/7, we must dig into our friendly capabilities, understand the operational environment, push the limits of technology, and work together to develop the tactics, techniques, and procedures (TTPs) that will win future wars. Training must continuously test us and our equipment. This struggle will prepare us to adapt to an ever-evolving enemy. Waiting is not an option. Our Army's ability to win the next war depends on our ability to collaborate, innovate, evolve, and adapt.

THE UNFORGIVING REALITY OF MODERN WARFARE

Our adversaries are already probing us and looking for weaknesses in our homeland cyber defense. They are building the tools to wage future war; integrated cyber teams, autonomous intelligence, surveillance, and reconnaissance (ISR) swarms paired with one-way attack drones, precision strike, and electromagnetic disruption capabilities. Many are designed to fracture our decision-making and paralyze our formations. Our nation must be ready. Our critical infrastructure must be resilient, not only to allow quick recovery, but also to enable our nation's ability to project power. Our Army and Joint Force must be prepared to rapidly take the fight to our enemies, on our terms, at a time and place of our choosing.

Imagine a typical Saturday night in a major U.S. city. The lights flicker, then the power grid collapses. Stoplights go dark. Hospitals switch to generators, which soon fail. Airports shut down. Trains stop. Emergency lines are silent. Meanwhile, hundreds of miles away, a division headquarters loses power. Communications are severed, and digital systems are locked. Military leaders are isolated. This is potentially the first act of a modern war, and it did not start with bombs, bullets, or missiles, but invisibly in the cyber domain.

Not only are the attacks we see in cyberspace becoming more complex, disruptive technologies are also affecting the land, sea, air, and space domains. Precision strike capabilities will change the way our Army conducts logistics and will push higher-echelon command and control (C2) further from the front lines. Unmanned aerial systems, artificial intelligence (AI)-enabled robotics, and ubiquitous sensors are already changing how tactical elements fight. Every day, battlefield systems get smarter and faster. Technology has placed data and communications links at the forefront of modern war. As our Army transforms to realize the potential of commercial technologies as force multipliers, we must ensure they are integrated with rigorous testing. Our adversaries are probing for every exposed port and vulnerability.

Our signal, cyber, and EW Soldiers must be ready to fight our way out of home station and enable our Army to deploy, fight, and win in LCSO. This integration is foundational to winning in tomorrow's battlespace. Our Army and Joint Force must have confidence in their C2 networks, even as our adversaries contest every frequency and data path. All cyber elements of war are in play. The side that controls the flow of information and data will set the tempo, shape the narrative, and set the conditions for victory.

TACTICAL CHANGE: TRAINING FOR REALISTIC SCENARIOS

Today's battlefield demands a radically different training paradigm. Our forces must rehearse under conditions that mirror the challenges of modern warfare; denied Global Positioning System (GPS) access, congested or compromised spectrum, and constant disruptions to C2 systems. By preparing for the worst, we empower our teams to overcome disruptions and outmaneuver adversaries.

At the tactical level, success requires formations trained to fight through disruption. In the dirt, company-level teams execute complex operations in GPS-denied, comms-disrupted environments using burst transmissions and analog mission command. Soldiers maneuver using maps and compass. Soldiers keep the mission moving forward by deploying software-defined networks, low-profile and mobile comms kits, adjusting frequencies, and autonomous link restoration tools—all under fire.

Tactical EW teams must identify and suppress enemy signals while feeding spectrum intelligence to squad leaders maneuvering through chaotic terrain, which can't happen unless units have trained in the worst conditions, against a cunning and capable OPFOR, over long durations that expose every friction point. That's how trust is built, systems are hardened, and leaders gain confidence to command in combat—not from theory, but from experience.

This kind of performance doesn't come from PowerPoint slides or sanitized training lanes. It comes from ten to fourteen days in the dirt, under constant physical and network stress—exactly what General Chris Donahue, Commanding General of U.S. Army Europe and Africa (USAREUR-AF), called for. It's why Army training must capture the friction and fatigue of real conflict—not simulations, but struggle. This is where the Army's edge is tested and proven. That's where trust is forged, systems are hardened, and confidence is earned.

We must harden systems at the code level and across the industrial base, as the Secretary of the Army has emphasized. Forces have to be trained to operate effectively with and without digital tools. Accreditation and red-teaming of all external software should be required before integration. We have to develop comms systems that don't broadcast position or intent, even while aggregating data, and maintain the capacity to project across the full spectrum—on our terms, at our time and place of choosing.

Project Convergence proves that we are able to connect sensors, shooters, and commanders across all domains—land, sea, air, space, and cyber. Project Convergence experimentation demonstrated progress in interoperability, targeting speed, and data-driven decision making. We now must continue to test those systems in scenarios and operational environments that mirror modern warfare, including the presence of OPFOR employing current or projected adversarial capabilities. Only then can we know that our tools and tactics are battlefield-ready.

Our Combat Training Centers (CTCs) provide some of our most realistic large-scale training environments currently available. At our CTCs, units experience tactical adversity, practice C2 in high-stress environments, and refine their ability to synchronize at scale. Use of advanced simulators, virtual reality, and OPFOR makes these centers the Army's premier proving grounds. However, CTCs cannot fully replicate the totality of modern warfare. Real enemy forces are dynamic, adaptive, and willing to disrupt or destroy the systems the Army relies on. Simulations, however advanced, do not replicate the constant pressure of cyber disruptions. CTCs also primarily train at the brigade level, which no longer aligns with the Army's shift toward divisions as the primary unit of action. The scope and scale of CTC training must grow—both in complexity and echelon—to match the scale of the multi-domain, cyber-contested nature of future conflicts. To successfully conduct the complex ground operations of modern warfare, our Army will be required to practice routinely with large units in the field under realistic conditions against a tough and creative OPFOR.

To close the gap between today's training and tomorrow's warfare, the Army must train in environments where C2 systems are denied, degraded, or disrupted. Future training should include exercises lasting up to two weeks in GPS-denied, spectrum-degraded environments to assess the true resilience and adaptability of units. This type of training provides invaluable insight into the performance of sensors, human-machine teams, and networks under pressure. It reveals whether systems are truly ready for combat conditions and whether commanders can still operate effectively without digital aids. As our adversaries become more capable in cyber and electromagnetic warfare, we must ensure our leaders and Soldiers can fight without the comforts of uncontested bandwidth and uninterrupted GPS.

The Army's transition to a data-centric force depends on developing leaders and building teams that are both technologically competent and tactically adaptable. In a world where AI and machine learning are informing decisions at machine speed, commanders must learn to integrate these technologies. Training environments must expose leaders to AI-assisted decision making and allow them to build familiarity and trust in machine outputs, while maintaining the ability to select, configure, and validate that AI tools are effectively and ethically employed.

Army scientists and engineers are already leveraging digital twins and virtual battlespaces to simulate the speed and consequences of algorithmic warfare. These tools must be

integrated into CTC rotations, ensuring leaders can interpret, trust, and act on machine-generated insights in time-constrained environments.

We must also rigorously wargame multiple scenarios across the full range of operations, involving different threats and geographies. Tactical decision games, field exercises, and mission rehearsals reinforce common reference points, enabling rapid communication and adaptation in combat. The Army must train not just to win the next fight, but to prevent the worst-case scenarios from occurring in the first place. Our Army must be able to defend the homeland from a cyberattack at the scale of a blackout scenario and at the same time, to fight in a congested and contested environment in a war scenario.

As much as technology is transforming the battlefield, war remains a human endeavor. Combat remains a contest of wills, requiring discipline, resilience, and leadership. Training must stress the cognitive limits of commanders and reinforce adaptability under pressure. Tactical decision games and immersive map exercises must accompany digital simulations to ensure that leaders and units can operate effectively in both high-tech and no-tech environments. Commanders must be trained to function when networks are down, sensors jammed, and communications disabled. Just as Soldiers are required to navigate with a compass and map, leaders must be comfortable operating without the digital tools they've come to depend on.

OPERATIONAL CHANGE: INTEGRATED TEAMS FOR UNIFIED STRENGTH

Both at home and abroad, we are under constant surveillance. Sensor war is here, 24/7. We are being watched, probed, and targeted. The global operational environment is connected and complex. We must stay ahead of the warp-speed evolution of modern warfare. Today's battlefields are defined increasingly less by physical terrain. Instead, they are increasingly encompassing the digital and cyber domains. The Army's ability to command, control, communicate, and resupply at speed—while securing its data and networks—has become as essential to victory as maneuver and firepower. In a sensor war, emissions control saves lives, and the element of surprise stems from deliberate activities that disrupt the enemy's ability to interpret our actions. Planning and maneuvering in the technical space enable our Army to seamlessly integrate signal, cyber, and EW capabilities across joint, theater, corps, and division formations.

Winning demands seamless convergence of cyber, EW, and signal capabilities across all echelons. Operational silos have long been our Achilles' heel and must be eliminated. We must act swiftly and decisively to unify our cyber, EW, and network operations, visualize the operational environment, ensure network resilience, and confront multifaceted threats in real time. Unification will facilitate Next-Generation Command and Control NGC2 and enable warfighters to access applications, analytics, and data tailored to the mission.

Signal Soldiers must enable uninterrupted C2 through spectrum-aware routing, agile waveform management, and diverse satellite communications (SATCOM) constellations, while cyber teams work alongside planners to identify and exploit enemy vulnerabilities in near real-time. EW platforms must conduct simultaneous denial and deception operations, shielding friendly networks from interference. Commanders must be empowered to coordinate joint fires and maneuver elements across vast distances with speed and confidence, even as adversaries contest every frequency and data path. This integration isn't optional. It's foundational to winning. Dominating the spectrum is no longer a supporting effort; it's a strategic objective. The side that controls the flow of information and data will shape the narrative, set the tempo, and define the conditions of victory. Our adversaries understand this and are investing heavily in capabilities that can isolate formations, degrade sensor-to-shooter speed, and interfere with or disable C2 networks. We must maneuver in the cyber domain to maintain the initiative.

Visualizing the operational environment is crucial for maneuvering in this technical space. As we harness the power of technology and innovation across all our battlefield systems, the number of connected sensors, battlefield systems, weapons, flying vehicles, robots, and other devices on the battlefield has exponentially increased. Our NGC2 is well-postured to achieve the real-time data throughput demanded by these technologies. However, as we leverage the advantages of emerging technologies, we must preserve capabilities that enable us to maximize full spectrum usage and resilient C2 and support activities.

“The combination of ubiquitous sensing and precision strike...pushes operational and strategic support area activities—logistics, staging, and higher-echelon command and control (C2)—further away or into distributed nodes.”

– General James E. Rainey
Commanding General
U.S. Army Futures Command

Achieving and maintaining positions of advantage across the battlespace is a complex task. Not only must we ensure the resiliency of our C2 networks, we must also manage and synchronize our land forces' broader use of the EMS. Spreadsheets are usually effective for managing the static allocation frequencies in our training environments, but that environment is becoming congested. We will deploy to environments where the EMS is congested by commercial activities and adversarial deployment of EW capabilities. Cyber and kinetic activities target our long-haul communications capabilities and data routing. As every warfighting function transforms—mission command, fires, movement and maneuver, intelligence, sustainment, and protection—and everything connects via the spectrum, the Electronic Warfare Planning and Management Tool (EWPMT) must be prioritized and evolved as a capability so we can effectively visualize, manage, and maneuver in this space.

To optimize employment of new concepts and capabilities, signal, cyber, and EW must collaboratively wargame all aspects and phases of operations. Our traditional approach towards communications PACE (primary, alternate, contingency, and emergency) planning must evolve to account for both the advantages of new technologies and the impact of degraded environments. Different routes and transport mediums must be synchronized in time and space to ensure network resiliency for mission priorities. Planning for autonomous robots, moving sensors, flying drones, and range bubbles for radios and EW capabilities occurs in three-dimensional space and requires consideration of a growing multitude of factors. Further complicating this is the nature of the constant and dynamic interactions between our forces and those of our enemy. Countering enemy sensors and precision strike capabilities requires emissions control (EMCON) and deception activities, which increase the risk of routing bottlenecks between our forward land forces and their higher-level support. We must build on the Army's running estimate of the future operational environment and get to the next level of detail for the EMS and data routing through intelligence-informed wargaming, research, and experimentation of network, cyber, and EW capabilities. Synchronizing the EMS and data routing in time, space, and purpose can only be realized through the combined efforts of our signal, cyber, and EW team.

“The Army Warfighting Concept is a living document, based on a continuously updated Running Estimate of the Future Operational Environment. This process includes intelligence assessments, observation of ongoing conflicts, research, wargaming, experimentation, and innovation by operational units deployed forward in their operational environment.”

– General James E. Rainey
Commanding General
U.S. Army Futures Command

This triad—cyber, EW, and signal—is no longer a support function; it is a core part of maneuver, fires, survivability, and dominance. Yet the tools of this triad that strengthen us, such as cloud aggregation, AI-enabled planning, and sensor fusion, also make us vulnerable. Too often, unaccredited tools—used for convenience—expose entire commands to infiltration. Adversaries know the easiest way to destroy a formation is to disrupt it before it even leaves home base. This isn't just a technology problem. It's a human one. The Army must reclaim proficiency in foundational tasks—manual navigation, analog communications, and terrain association—because in the next war, the first thing we'll lose is connectivity. The Army's success depends on Soldiers who are well-trained in chaotic environments and able to function independently in the most degraded conditions. We must protect and maintain our cyber, EW, and signal tools as the weapons systems they have now become.

STRATEGIC CHANGE: EVOLVING RESILIENCE AND INNOVATION

The United States Army is at a critical point. The accelerating pace of technological change, the emergence of new domains of warfare, and increasingly complex and contested operational environments demand swift, decisively implemented reforms. Reform must be a priority, or we risk operational failure and the loss of American lives. If we fail to implement the needed changes, our Soldiers will deploy with inadequate equipment, insufficient training, and a legacy mindset ill-suited for modern warfare. Without advanced sensors, systems-of-sensors, and the ability to disrupt the enemy's sensor and targeting networks, our forces will be exposed and unable to hide, maneuver, or strike effectively. In denied environments, where GPS and communications are compromised, untrained and unequipped formations will falter, and people will die.

Brigade commanders must win the close fight with integrated sensors and fires, while division and corps leaders must visualize and control the operational depth across domains. Data analytics must empower decision-making at every echelon, and cybersecurity must shield these digital capabilities from attack. The rise of data-, software-, and sensor-centric warfare requires every Soldier to understand how data is collected, used, and manipulated, and how to fight in a world shaped by information advantage. Delays in implementing reform will cede the advantage to our adversaries and place our Soldiers—and our national security—at risk. Continuous investment in technologies, people, and ideas is imperative.

Outpacing adversaries requires us to overhaul how we resource and equip our forces. This includes prioritizing resilient, secure, and adaptive capabilities and communications systems. Rapidly advancing technology means emerging threats will evolve faster than ever. Investing in innovative solutions will allow us to maintain the edge.

The Army's ability to project communications and cyber dominance under pressure reassures allies and deters adversaries. Army leaders and planners must intensify efforts to build theater-wide network redundancy, enable assured access to shared space-based assets, and harden global data transport layers.

Failure to institutionalize training in realistic, hostile, and denied environments will result in commanders and units being unprepared for the chaos of multi-domain operations. Our inability to detect, visualize, and strike at range will allow adversaries to dictate the nature of the next war. Integration must happen at the speed of software, not bureaucracy. Our Army's leaders must be empowered with training, tools, and the right force structure.

Our policies must align with a process that enables Directive Authority for Cyberspace Operations (DACO) to clarify who has authority in the cyber domain in each area of operations. In the Continental United States (CONUS), U.S. Cyber Command (CYBERCOM) has authority. However, when a unit deploys, it remains unclear as to when authority transfers from CYBERCOM to the regional command (e.g., USAREUR-AF).

We also need policies that expedite the relief in place and transfer of authority (RIP/TOA) process and clarify MPE cyber authorities more effectively. The handover of cyber, signal, and EW responsibilities and capabilities between outgoing and incoming units in deployed locations should be far more seamless, accelerated, and fully complete by the time the change of command ceremony takes place. Mission partners also bring cyber capabilities to the fight, and policies are needed to better enable unified action and C2 across domains with allies.

Continued investment in cyber, signal, and EW capabilities—alongside organizational reform and talent development—will ensure the Army has a unified, agile, and empowered digital force that dominates across all domains. Each investment should be evaluated as part of a broader force transformation plan that integrates all warfighting functions. To achieve the Army's 2030 Vision, we must continue reshaping how the Army learns, trains, and fights.

CONCLUSION: HARNESSING COMMUNICATIONS AS STRENGTH

Many elements of the future fight are already upon us. Now is the moment to decide whether we will adapt or let ourselves be outpaced. The next fight won't wait for us to catch up, and it won't resemble the battles we've grown comfortable preparing for. It will be contested from the first byte to the last bullet, fought in shadows, across the entire spectrum and every domain, and under relentless pressure from persistent, intelligent, and networked adversaries.

On the modern battlefield, data and communications are vital to the success of all operations, driving our ability to sense, decide, and act faster than our adversaries. Our ability to operate, disrupt, deceive, and dominate across that battlefield depends on whether we learn lessons at warp speed before our enemies adapt. Without urgent innovation, our greatest strength could become our greatest vulnerability. Signal and cyber warriors—those who enable our data dominance—could become overly constrained by outdated systems, inadequate training, and legacy thinking. The choice is clear: evolve now or be outpaced by adversaries who will force us into reactive, costly, and deadly catch-up.

From the legendary Greek who ran from Marathon to Athens to deliver news of victory, to Paul Revere's midnight ride to warn of an impending attack, history reminds us that early detection and rapid dissemination of information have long been the foundation of defense, and often the only difference between victory and defeat. Today, data-, software-, and sensor-centric warfare is the modern equivalent—delivering critical awareness at the speed of relevance. This only works if we build and rapidly deploy secure, resilient, and redundant communication and sensor networks, supported by AI, as quickly as we can.

At its core, the backbone of modern warfare is data and communications. These elements offer unrivaled potential—both as tools of strength and as vulnerabilities to exploit. If we embrace the urgency of innovation and adaptation now, we can prevent our communications

and networks from becoming targeted liabilities. We hold the power to transform how we fight, how we defend, and how we prevail in battle that is, unequivocally, here and everywhere, 24/7.

If we are not preparing for the worst day—the day when communications are denied, cyberattacks paralyze systems, and adversaries strike across multiple domains—then we are not preparing at all. We cannot afford to rehearse for yesterday’s war. The era of uncontested battlefields is over. If we train, exercise, and experiment only in permissive environments, we will send unprepared forces into unforgiving fights. Victories won’t always go to the most connected force, but rather, to the one that can survive without connection. Adversaries know they don’t need to face our superior weapons if they can exploit our weaknesses.

We must never merely hope that our systems will work when they are needed. The Army must know it can win—even when they don’t. Readiness must be measured not by simulations, but by sustained performance in degraded, contested conditions. The Army’s digital edge must be matched by its analog resilience.

The challenge to Army senior leaders and policymakers is clear: commit to transformative change now. Everyone—Soldiers and scientists, engineers, intelligence analysts, acquisition professionals, lawmakers, academia, and industry—has a role on the front lines of this transformation. We must out-adapt, out-innovate, and outlast our adversaries in prolonged conflicts that will not only test our warfighting functions, but also our national will.

The Army must be confident that it will prevail amid total chaos. Our readiness will not be measured by what we accomplish in controlled environments, but by what we can sustain in the harshest, most unforgiving conditions, because in the next war, resilience—not convenience—will be the difference between victory and defeat. In the coming battles, it won’t be the side with the most drones or bandwidth that wins. It’ll be the side that knows how to survive and thrive when none of it works. Victory in future war hinges not just on firepower, but on information assurance and digital dominance. Cyber, signal, and spectrum dominance isn’t a supporting role—it’s the new strategic high ground.

ACKNOWLEDGMENTS

The author is deeply grateful to all who contributed to this article for their valuable insights, to include General James Rainey, Commanding General, U.S. Army Futures Command; General Christopher T. Donahue, Commanding General, U.S. Army Europe and Africa (USAREUR-AF); Sergeant Major Kristie Brady, Sergeant Major, Deputy Chief of Staff, G-6; Chief Warrant Officer 5 Rylan Knight, Chief Technology Officer, Army Deputy Chief of Staff, G-6; and Dr. David Markowitz, Chief Data and Analytics Officer, Office of the Chief Information Officer.