Persistent Surveillance and Its Implications for the Common Operating Picture

Major David W. Pendall, U.S. Army

THE IDEA of persistent surveillance as a transformational capability has circulated within the national intelligence community and the Department of Defense (DOD) for at least 3 years.[1] Persistent surveillance, also known as persistent intelligence, surveillance, and reconnaissance (ISR); persistent stare; and pervasive knowledge of the adversary, is an often-used term to describe the need for and application of future ISR capabilities to qualitatively transform intelligence support to operational and tactical commands.[2] The idea surfaces in many forms, including defense program reviews and congressional testimony.[3] Each expression envisions a system achieving near-perfect knowledge and removing uncertainty in war.

Persistence means that when global, theater, or local reconnaissance finds something of intelligence or actionable interest, ISR systems, including processing and analytic systems, maintain constant, enduring contact with the target. This increases understanding about the target, which enables a faster decision cycle at all levels of command and supports the application of precision force to achieve desired effects.

Persistent surveillance integrates the human component and various technologies and processes across formerly stovepiped domains; it is not a permanent stare from space or from airborne imagery platforms. In essence, the targeted entity will be unable to move, hide, disperse, deceive, or otherwise break contact with the focused intelligence system. Once achieved, persistent ISR coverage will, in theory, deny the adversary sanctuary, enabling coherent decisionmaking and action with reduced risk.

Persistent surveillance in its objective form does not exist today; it is still a concept, albeit a promising one. The promise of a persistent ISR system is to create transformational conditions for acting against the adversary within the battlespace. Whether or not nearly perfect knowledge is possible across multidimensional battlespaces with multivariant actors is a contextual and situational question. Even so, persistent surveillance will increase knowledge and the speed with which the knowledge is shared and understood at all levels of command, provided the system is developed in a holistic manner that addresses human, organizational, and technological aspects of the strategy.

Will Persistent Surveillance Change Battle Command?

Integrating persistent surveillance with an Information Age common operating picture (COP) will dramatically increase the potential to transform warfighting and peace management. Continuous sensing of the battlespace; a fundamental reordering of information distribution; and advanced, integrated sensemaking will create asymmetric advantages for the United States. Recognizing the global nature of the protracted challenges we face, a coherent national defense system must embrace a new means of control, one that can reorder information flow and move actionable intelligence and analysis directly to the individual level.

Persistent surveillance represents a qualitative change in the content and delivery of intelligence to those at the operational and tactical levels of war, a change that increases the speed of decisionmaking across all battlespace domains and at all levels of conflict, thus multiplying the options for applying both kinetic and nonkinetic force.[4] The qualitative change will evolve with and leverage a revolution in intelligence affairs.[5]

With persistent surveillance, sequential analytic and distribution rules become obsolete. Higher echelon analysts will no longer get the data first,

but in parallel with users, including those at the lowest levels of organizations. Analysts will not simply send reports to those they believe require the information; rather, the end user will define the information required, demand it, and be able to create the knowledge directly. Users will define information requirements based on specific decisionmaking needs and planning horizons. Serialized reports will become secondary; collaboration and a focus on user real-time support will become primary. Networking tools will connect analysts with other analysts, analysts with end users, and end users with other end users. A "smart" pull system will support all entities on the network, and lower level users will access relevant data as it is generated in real time.[6] Advanced preprocessing tools will support the user immediately in a variety of user-defined, immediately usable formats—all done in parallel to other networked users.

The Essence of Persistent Surveillance

The essence of persistent surveillance is to use enterprise systems to detect, collect, disseminate, and characterize activity in the battlespace. The recognition of anomalies or change measured against an established baseline will prompt action from decisionmakers. Persistent surveillance has three core components:

• Multimode and multidimensional continuous collection across all battlespace environments (sensing).

• Near-real-time data and knowledge distribution via enterprise systems with tailored, user-defined presentation formats (delivery).

• Horizontal integration of data and advanced, distributed analytics (sensemaking and understanding). (See figure 1.)

Persistent surveillance will create enterprise (intelligence) data and understanding to support an extended operational enterprise. "Enterprise data," "enterprise systems," and "extended enterprise" are information-management concepts emerging from the increased capacity of digitized information and distribution networks, namely the World Wide Web,
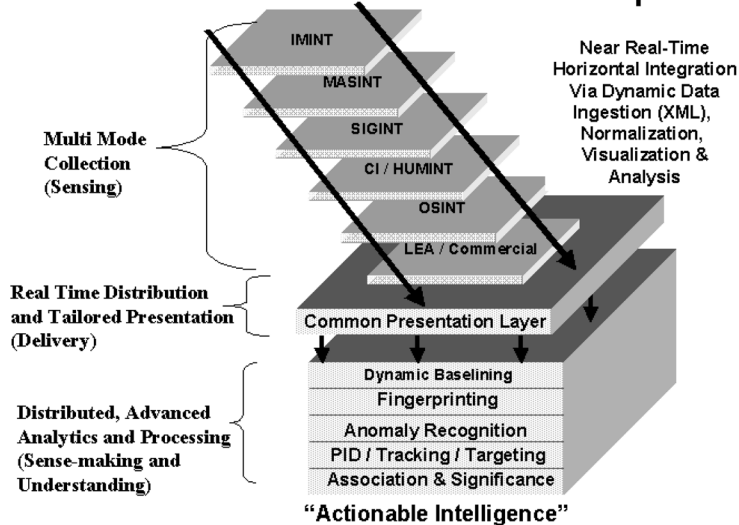

Figure 1. An integrated concept of the core components of persistent surveillance. Processing occurs within Knowledge Advantage Centers. Virtual or actual collaboration with analysts or automated processors or preprocessors supports edge users with real-time intelligence and allows users to access raw data at the earliest point of consumability. (Concept slide adapted from MG John F. Kimmons, U.S. Army Intelligence and Security Command, presentation at the Global Intelligence, Surveillance, and Reconnaisance Conference, sponsored by the U.S. Strategic Command, Denver, Colorado, 29 September 2004.)

virtual private networks, and industry intranets.[7] These concepts allow simultaneous access and use of enterprise data generated from internal and external organizational environments, enabling a friendly networked element to leverage knowledge rapidly at the point of competition.

Examples of enterprise systems include mobile, networked sales representatives leveraging dynamic sales and inventory data to make pricing decisions when negotiating with current or future customers; air traffic controllers collaboratively assessing severe weather effects on regional airports, then making rerouting decisions and impact assessments in near-real time; and point-of-sale transaction systems with above-normal sales levels generating a supply-chain response to restock shelves quickly at local stores without requiring unnecessary human intervention, thus reducing system latency.

The new rules firmly acknowledge the need to maintain persistent coverage capability against all threats, whether they are nation-state, non-nation-state, or transnational. This capabilities-based approach, unlike the Cold War threat-based approach to designing defense systems, recognizes the requirement to wage war and peace at the individual human or "entity" level, a re-conception that transforms the reconnaissance paradigm of snapshot views and periodic samplings. Persistent surveillance means longer

term collection on a target to completely understand a problem. This change will provide more data and continuity to analysts and warfighters.[8]

ISR logic co-evolved with that of our enemies during the Cold War. The new logic evolved after 9/11 as a "new rule set" for success against a massively distributed, decentralized global adversary.

Implications for the COP

The integrating mechanism to create a complete capability is the COP, "a single identical display of relevant information shared by more than one command."[9] The COP is also an enterprise information system, supporting an extended operational enterprise beyond DOD.

In a highly distributed information environment, a single COP display might remain appropriate if the information distribution moved hierarchically and the information remained static for periods of time. However, the single identical display creates its own problems when the future COP becomes a real-time enterprise information system supported by a continuous-data environment. Single identical displays are less useful than displays created dynamically for specific missions and domain views of the battlespace. As the Joint Forces Command study on the collaborative information environment (CIE) finds, collaboration capabilities allow users to tailor COP displays yet maintain common, relevant aspects of the operational picture.[10] The study also finds that a real-time environment significantly increases the COP's value if the user can define and dynamically tailor the views.[11] The key word is "if." We must transition to a COP with a dynamic tailoring capability to support real-time operating requirements and future planning requirements.

The COP must enable adaptive planning across planning horizons to achieve coherent, systemic effects. Complex systems survive by anticipating the future.[12] A transparent, tailored, integrated COP supports this anticipatory function. Each domain and level of war has echelons and suborganizations regardless of how flat a networked force becomes. Each level must operate within the appropriate time horizon. Parallel levels of war and parallel domains must remain nested in purpose, and enterprise behaviors are driven by intent. Effects can transit multiple domains and levels of war instantaneously, so purposeful adaptations through effects-planning must be thoroughly integrated.

Platoons, squads, and individual actors focus on real-time execution. Higher, more complex organizations focus on setting conditions for the future. Companies and battalions live in the near future, 12

to 48 hours ahead of the adversary's decision cycles. Brigades and divisions might live in the 48- to 96-hour future. Joint task forces and national decision-makers must create advantageous conditions beyond the 96-hour mark.[13] With a coherent, COP-enabled view of the planning horizon and persistent surveillance of adversary systemic changes, tempo control and effects-sequencing will provide the desired shaping and battlespace depth that units need to conduct operations. Enterprise planning systems help produce competitive advantage.

Examples of enterprise planning systems integrated with real-time data and anticipated change include the National Weather Service, which uses real-time weather data and advanced simulations to anticipate hurricane effects so local officials can issue alerts, conduct highway traffic flow analysis, and establish evacuation priorities. The U.S. Forest Service uses real-time weather data and forest fire simulation models to dynamically adjust its assets and plan with far greater insight about the scope and emerging conditions of a problem. Wal-Mart uses environmental, social, and cultural data to forecast and adjust inventories.[14] By identifying and generating options, anticipatory planning can streamline the decision cycle.

Developing and supporting proactive, option-seeking behaviors and exploitation-capable frameworks is difficult under current ordered, linear, deliberate planning constructs. In today's process- and plan-centric execution models, commanders often become prescriptive in intent, creating reactive tactical plans because of the perceived need to plan in detail for anticipated conditions. Rapidly shifting enablers across dispersed battlefields is problematic and adaptation is slow, especially at the operational level. Ordered, mechanistic, linear thinking limits the ability to capitalize on options and exploit new conditions created at the tactical level. Deviations from the anticipated, and an appreciation of new, unpredicted, and continually emerging circumstances, led Prussian General Helmuth Von Moltke the Elder, to view strategy as a system of expedients (options) and to caution that plans should only go as far as the first encounter with the enemy.[15]

Commander's critical information requirements (CCIR) filter information and allow humans to better synthesize it to support decisionmaking. Decisions are forecast in advance, often based on assumptions. Where information systems find and report the required elements to support CCIR, other information, which could lead to new, improved decisions and superior execution, often falls outside the scope of "the plan" and is not seized on. For all the

commander's admonishments to "fight the enemy, not the plan," staffs often present only information that supports or denies the plan's key elements. Brigadier General Huba Wass de Czege writes: "Anticipatory planning and adaptive execution can address the unpredictable will of the enemy and the chance factors which make forecasting the future difficult regardless of how much information we possess. . . . The object is to achieve sound, adaptable, simple and decisive plans based on the best available information, understood and coordinated . . . so that vigorous teamwork can produce the desired results. . . . Shared understanding and anticipatory planning combine to produce adaptive execution, which is the systemic ability to adapt plans to emerging situations in time to ensure continuous deliberate operations. . . . New planning and execution systems will be needed to implement this process.[16]

An execution-centric model with real-time intelligence to identify and predict changes in enemy systems will create new information, reduce operational risk, and enable bold option exploitation. U.S. Army Field Manual 6-0, *Mission Command: Command and Control of Army Forces,* which calls such information exceptional information, states: "Exceptional information is specific and immediately vital information that directly affects the success of the current operation. It would have been one of the CCIR if it had been foreseen; it is therefore treated as one of the CCIR. Exceptional information usually results [from] discovering something unanticipated about an enemy. It allows the commander to take advantage of an unexpected opportunity. . . ."[17]

Exceptional information increases when persistent surveillance capabilities integrate into the COP, particularly as near-real-time effects-sensing generates feedback. Enemy system adaptations become more clearly identified. An operational paradox emerges, however, because tightly coupled, detailed elements (the basis for synchronization) often make large shifts in execution infeasible.

The multiple, simultaneous, distributed, decentralized nature of combat operations that joint operating concepts describe requires commander-led, execution-centric planning. Collaboration tools in a CIE allow parallel planning to move away from the ordered, timeline-sequenced actions described in Joint Publication 5-0, *Doctrine for Planning Joint Operations*.[18] After-action reviews from Operation Iraqi Freedom indicate Force XXI Battle Command System Brigade and Below's collaborative capabilities are already supporting moves in this direction. Executing multiple, simultaneous, distributed, decentralized actions requires relevant operational information fusion across all levels of command and in presentation formats accessible to all, including multiagency, civil, and coalition partners.

Reordering Information Distribution

With persistent surveillance, information pathways will move information directly to collaborative users (rather than through successive headquarters) and empower all echelons, given the right tailoring of the COP. Real-time data distribution will transform all previous information-control mechanisms across the joint force and its partners.[19] An enterprise COP means "exclusivity of data is not the defining attribute of decision."[20] An extended operational enterprise relies on multiple, decentralized, and distributed actors to achieve its purpose.

The agent or actor is any individual, individual element, or entity that can interact with its environment to create effects against other actors and the environment.[21] From a single rifleman to a Tomahawk missile, from a policeman to a Computer Emerging Response Team, agents exist throughout the domains of conflict and levels of war, all interacting to create effects across each domain and level of war.[22]

Under current information dissemination architectures, the means of control coexists with levels of command. To synchronize action at the various levels of war, information is rationalized and integrated with direct, centralized command guidance. With an enterprise data-generation system, including direct dissemination capabilities, COP control parameters must change. Control mechanisms remain the means of regulating behavior, as they always will, but in the 21st-century COP, they will move from centralized command nodes to distributed processing nodes, which become Knowledge Advantage Centers (KACs).[23]

KACs enhance self-organization, self-synchronization, and self-empowerment down to the lowest levels. The Army endorses this in the "2003 Transformation Roadmap": "A focal point of DOD's thrust to fully exploit network-centric warfare is the development of persistent surveillance. In support to this goal, the Army will develop supporting persistent surveillance capabilities throughout the global battlespace. This provides the commander near continuous access to the priority intelligence targets. The objective is to develop network-sensing suites that tailor their observations to the adversary's rate of activity. The goal is to combine the broad spectrum of current and future sensors into an effective intelligence tool that is geared to the activity of an adversary. The amassed information is input into an

Reconnaissance	**Persistence**
• Periodic, "snapshots" in time	• Continuous, enduring contact and "dwell."
• Stovepiped, hierarchical collection.	• Multimode collection with broad access.
• A few sensors support a few missions	• Sensors support entire enterprise
• Analysts see data first and pass	• Data available across network to all
• Target-centric collection and analytic focus.	• Deep systemic and relationship focus.
• Analytic templates and assessment.	• Patterns, inference, case-based models.
• Data sets remain within stovepipes	• Data integration—horizontal and vertical.
• Driven by predetermined requirements.	• Data and analysis on demand.

Figure 2. A paradigm shift: From reconnaissance to peristence.

Internet protocol where it is universally available to all warfighters. *This approach involves a paradigm shift in how raw data is entered into the network. Instead of analysts processing raw data into information for input into the network, the raw data will be placed on the network for empowered users to exploit for their own particular requirements. The decision on what is important moves from the entity that captures or analyzes the data to the person who uses it"* [emphasis added].[24]

Animated and three-dimensional presentation will allow users to understand specific mission sets and effects-generation. Current tools, such as Topscene and Falcon View, allow combined domain views, such as a synthesis of terrain data with the infrastructure views of the signal or information environment. Future tools will increase the value of enterprise data, creating an even greater ability to perceive each domain's dynamic environment.

Right now, the logic driving most service and joint ISR is the Cold War reconnaissance paradigm: periodic, linear snapshots and samplings.[25] The logic reflects the adaptations and co-evolutions of the past and is increasingly inadequate for the future. (See figure 2 for a summary of the differences between the reconnaissance paradigm and the persistence paradigm.)

We must consider the emergence of persistent surveillance in the context of future combat and national-security capabilities, and as such, persistent surveillance should be nested in the higher operational capability it serves. Form follows function. The guiding vision—a globally coherent national-security system—requires a coherent operational system to exercise all elements of national power.

Distributed Effects Over Time

With decision distribution, operational art becomes a fully collaborative exchange, and leaders and planning staffs primarily focus on operational tempo, set conditions through anticipation, and describe desired effects. In the past, effects ran concurrently with battlefield actions, but distributed, decentralized operations create asynchronous effects. Tempo control and effects-linkages across the levels and domains of war affect the adversary in time and space. For example, logistics preparation and movement of actors are often indicators and precursors of action. With persistent surveillance, we identify enemy precursors and act on them in a greater variety of ways. We might delay or prevent collusion, seize key assets or finances, or deny commercial transportation means. Each action increases friction and reduces the enemy's operational capacity, which creates an internal focus that continuously forces him to adjust his plans. We achieve a temporal advantage by creating deep, systemic effects. Tempo control becomes the most important element of operational art.

An integrated COP environment supported by persistent surveillance will enable commanders to create tempo through effects planning. Control will be indirect. Commanders will direct KACs to alter mission parameters and effects sequences. Mission formation will take less time because key players

will collaborate to construct effects elements in each domain and level of war. Collaboration begins with a shared understanding of the commander's effects-based intent.[26] The objective must be clearly defined. Lack of purpose to provide context to an effects-based intent results in incoherence.

Mission command at lower levels will be established through self-regulating behaviors and self-organization, all related to mission purpose and clear intent. Rule sets will outline a maximum-minimum behavior set to follow.[27] A commander then takes in information, makes judgments, and directs subordinates as situations change. In a distributed-enterprise COP, a commander's direct intervention will be greatly reduced because subordinate actors and systems will collaborate to generate desired effects. Commanders will lead from the center of the network (rather than from the top as in a hierarchical organizational structure), provide umbrellas of enabling resources, and ensure freedom of action. The commander will also fight to extend the view deeper into the battlespace so he can determine how to shape the environment and create broader options. Self-synchronizing actions will occur in parallel, distributed operations in each domain and at each level of war, but even in execution-centric environments, purpose remains the most important element.[28]

Achieving Coherence

Coherence of action and continuous operations will require a program-management mindset and a long-term view of decisive operating advantages and conditions, not a project-management mindset focused on producing activities of transitory usefulness that support a single end state. Coherence will come from correct effects design (supporting a larger purpose) and tailored information distribution, not direct controls over single actors.

Because of a lowering of what constitutes the operational level of war, lower level actors will face diverse response requirements as they integrate with other actors in the battlefield. Today's battalion commanders often deal directly with non-DOD elements in ways a corps commander might have 15 years ago. As one senior joint force commander emphasized: "There are nearly 30 interagency elements operating in Iraq today."[29] A senior Army commander added: "[There is] only [an] illusion of control. Consider the integrated operations of SOF [special operations forces], Interagency, Coalition and [nongovernmental operations]; [military commanders] don't really own it [their battlespace]—this is real."[30] What the contributing effects are, or should be, must begin with a common understanding of the adversary as a system.[31]

Coherence includes purposeful combinations of kinetic force, arrests or seizure of material and funds, nonkinetic efforts through computer-network operations or the initiation of public diplomacy, and messages disseminated through global media to shape perceptions. Some actions might not be military in nature, but military commanders might coordinate and develop plans for nonmilitary actors to execute in order to create necessary effects. Such actions might include acting through interagency partners and nongovernmental actors, with or without attribution to the military command.[32]

The Major Combat Operations-Joint Operating Concept states that joint force commanders will find themselves increasingly engaged in peer leadership outside the organizations they command and control.[33] Lower echelon commanders will find themselves in similar situations as their forces increasingly act in complex environments as we prosecute the Global War on Terrorism.[34] In short, the need to create unity of purpose and coherence of all effects in the operational environment has expanded. Each effect adds to the desired outcome, creates continuous pressure, and changes the enemy's decision cycles. Moreover, because of an increased ability to identify key relationships and vulnerabilities across an enemy's global operating systems, effects might be initiated in many operational areas that create desired effects in others, and vice versa.[35]

A COP supported by distributed persistent surveillance is also likely to support actions against precursor behaviors, adversarial collusion, and physical or virtual node associations. Cumulative effects can pre-empt or diffuse conditions requiring lethal force. By denying the enemy opportunities, we also deny him key conditions for success.[36] Effects-based operations are outcome-based and do not depend on a particular organization to generate input. In the past, the focus of intelligence was on named areas of interest, a term nearly meaningless in a persistent surveillance paradigm. The new term is "named relationships of interest." As the enterprise mind gets stronger, we become increasingly able to predict events, our actions become more preventive, and we reduce the use of lethal force.

Magnetic resonance imagery (MRI) is a form of persistent surveillance in the medical field. Affordable scanning has produced more frequent imaging and improved the evidentiary base that, in turn, has allowed case-based reasoning and inference models with which doctors could compare a single patient's results to previous scans as well as anomalies to the base. As the data built a greater understanding of the disease, doctors could identify precursor attributes

Airman preparing to enter a building during an urban warfare exercise. The exercise was conducted to test integration of a Scan Eagle unmanned aerial surveillance aircraft.

leading to definitive cause and effect linkage. As a result, preventive medicine and treatment options grew tremendously. More effective use of medicines and chemotherapy (nonkinetic treatments) led to increased survival rates. With image-guided surgery, doctors could operate with more precision, because MRI devices scan in real time during surgery (kinetic treatment).[37] The COP should allow a similarly precise and effective use of force across the battlespace.

Exploitation is an operational term. In the past, cavalry created the next battle and exploited success. In the Napoleonic era, there was no deep cavalry because there was no next battle. Industrial Age commanders formed cavalry when they realized that a single, "decisive" battle would not end a war. Now we see continuous operations and global (small-unit) battles. In the future, the cavalry might not exist as an organization, but as a global sensing system of systems; that is, as persistent surveillance and agents conducting exploitation operations.[38] However, just as cavalry reporting is not perfect, neither is persistent surveillance.

Recommendations

Persistent surveillance will enable the Joint Operations Concept's (JOpsC) attributes and result in new organization, strategy, and authority distribution.[39]

Leaders, actors, and agents will adapt through training, simulation, and experiential learning to create new operational values and cultures.

Perhaps the most significant noninformation technology-related effect from integrating the emergent persistent surveillance capability into the COP will be on human capital and security organization design. Rethinking training models, leadership skills, and retention requirements, and better leveraging of individual experiential factors, will help achieve the broad security and operational goals JOpsC outlines.

Training. We must incorporate collaborative problemsolving and simulation to reinforce recognition-primed decisionmaking at platoon, squad, and team levels. We must use physical and virtual scenarios with dynamic mission changes, rule sets, and authority modifications as scenarios unfold and distribute changes to the force through individualized COPs. Physical-skills training for close-combat operations should incorporate real-time COP feeds and advanced technologies as soon as spiral insertions allow, as we practice connecting soldiers and entities to the network. Training should reinforce adaptation, virtual and physical collaboration, and mental agility within the mission set. Operational-level training should focus on operational design and planning for parallel, distributed actions, using

The TPS 75 Air Surveillance Radar System at Aviano Air Base, Italy, 5 October 2005.

dynamic systems thinking as a basis for a new military science.

Leadership. Shared persistent surveillance and an integrated COP will require leaders who are comfortable with exercising indirect control over decentralized missions. Leaders must also develop enhanced skills in peer leadership and informal leadership of non-DOD elements within the battlespace. Battlespace visualization and understanding increasingly comes from the COP, not a single commander. No single commander is likely to understand all the complexities and necessary, tempo-sensitive interactions within the battlespace, particularly "on the edge" events during tactical operations. Leaders at battalion-level and below should receive enhanced training to handle greater authority. Those who can achieve effects should have the authority to do so. Organizational leaders should develop around dynamic systems and enterprise leadership models. Senior leader training should teach how to influence and indirectly control distributed operations through adaptive mission planning and effects design communicated through the commander's effects-based purpose and intent.

Experience. We must improve retention incentives and nurture operational experience. An enterprise mind-enabled force having an integrated COP and persistent surveillance feeds requires enhanced skill sets and increased levels of maturity. We also need to leverage the collaborative skills of information-technology-savvy soldiers who are comfortable with pervasive communications and computing technologies. Junior leaders and soldiers have shown tremendous adaptability during Operations Iraqi Freedom and Enduring Freedom. These soldiers are bloggers, on-line gamers, smart mobsters, and chat-room influencers. Future tactical engagements might primarily be at the platoon and below levels, with a brigade combat team (BCT) headquarters serving as the enabler and integrator for dispersed companies and platoons. Even SOF elements might break into individual and split-team operations and work ever more closely with interagency partners. The United States has the most experienced, educated Armed Forces in its history, and our Nation's future will require leveraging our best in this protracted war.[40]

Organizational design. New organizational constructs should also emerge, with authorities following information flows and an expanded capacity to act. Because strategy is reflected through organizational design, force designers should continue to emphasize empowerment of formations at company through team levels and the interaction of conventional and special operating forces. Future force designs should continue to emphasize soldier and soldier-level empowerment. Enablers for integrating force, whether the force is from interagency, multinational partners, or the joint force, should be the product of coherent operational design and planning

from the joint task force through BCT levels, with emphasis on shaping and condition-setting. With enhanced COP capabilities and a more direct flow of information resulting from the changed, distributed nature of information enabled by persistent surveillance, it is unclear what the role of the division headquarters G2 might be.[41] Theater- and national-level planning must focus on deep, global operations and long-term success in protracted war.

Experience levels. Increased complexity will require seasoned leaders and mature staff in battalion and below combat formations. Leader-to-led ratios must increase. Companies should have intelligence sections to fully leverage persistent intelligence distribution and enable tactical planning beyond immediate engagements. We must track and manage intangible assets across the force; namely, specific experience, specialized skill sets, and demonstrated proficiencies. Each of these suggestions raises the operating capacity of edge organizations and empowers the lowest levels of the force to act with speed and precision.

Force structure. We also must create an integrated force structure that combines special operations elements; rapid, strike-capable conventional elements; and deep operations forces, including interagency teams. These forces should engage in theater security and cooperation initiatives and operate with specialized rules of engagement and authority to create preemptive or preventive effects. This force would likely have the agility and judgment to be a shaping force for global operations that can intervene decisively to prevent larger crises from forming.

The COP. The spiral development and integration of information technologies can provide the force with an asymmetric capability if technologies are integrated correctly with the human component. The COP must allow—
- Access to all mission elements and to real-time

enterprise data via the tailored COP with assurance in content and reliability.
- Mounted and dismounted support to extend support to individuals, rather than just platforms or command posts. We must ensure COPs reach DOD and non-DOD partners. Tailorable COP designs should support dismounted operations in remote areas just as seamlessly as they support a teammate in a hotel room operating in dial-up-access mode.
- Robust planning and simulation tools that reside on-line and allow users to integrate real-time data with planning products automatically. Tactical planners should be able to integrate the same enterprise data into tactical simulation and visualization tools to create dynamic mission-rehearsal and tactical-analysis visualizations.
- Layered security and smart distribution, so support users can operate securely within their mission environment and the appropriate planning horizon.
- Reinvention of display and visualization because one size does not fit all. We must allow users to design and test new COP presentation displays for anticipated operating environments. There might never be an end goal to build to, but rather a steady move to bring understanding to the individual through continuous advances in technology.

Integrating persistent surveillance with the COP allows us to reconceive security mechanisms to meet today's threat. Today's threat is not regional but global, mobile, and intertwined with civil and even commercial infrastructures. We must leverage persistent intelligence to meet our requirements through a shared COP that supports the police sergeant as well as the Army sergeant with relative, actionable data. We must also create mechanisms and technologies to allow broader access to non-DOD and non-U.S. elements based on the mission. A multinational-capable, tailored COP would foster global agility and coherent actions. *MR*

NOTES

1. Office of the Secretary of Defense, "Transformation Study Report: Transforming Military Operational Capabilities," Executive Summary, Washington, D.C., 2001, 2, on-line at <www.defenselink.mil/news/Jun2001/d20010621transexec.pdf>, accessed 31 October 2005.

2. Terms such as persistent or pervasive denote the same basic operational capability. I Corps Commander LTG James M. Dubik used the term pervasive knowledge during a lecture at the U.S. Army School of Advanced Military Studies (SAMS), Fort Leavenworth, Kansas, on 4 October 2004. The concept is consistent with the concept of persistent surveillance.

3. Donald H. Rumsfeld, "Quadrennial Defense Review Report," Office of the Secretary of Defense, Washington, D.C., 2001, 30, on-line at <www.defenselink.mil/pubs/qdr2001.pdf>, accessed 31 October 2005. See also Stephen A. Cambone, "Statement of Dr. Stephen A. Cambone, Under Secretary of Defense for Intelligence, before the Senate Armed Services Committee, Strategic Forces Subcommittee,

Intelligence, Surveillance and Reconnaissance," Office of the Under Secretary of Defense—Intelligence, Washington, D.C., 7 April 2004, 4.

4. The battlespace includes three competitive domains: physical, informational, and cognitive. These domains are also distributed among the three levels of war: strategic, operational, and tactical. See David S. Alberts, John Garstka, Richard E. Hayes, and David T. Signori, *Understanding Information Age Warfare* (Washington, DC: Command and Control Research Program Publication, 2001), 10-15.

5. VADM Lowell Jacoby, "Revolution in Intelligence Affairs," presentation at the Armed Forces Communications Association's Spring Intelligence Symposium, Langley, Virginia, 22 April 2004.

6. Alberts and others, 120.

7. Kenneth C. Laudon and Jane P. Laudon, *Management of Information Systems: Managing the Digital Firm*, 7th ed. (Upper Saddle River, NJ: Prentice Hall, 2002), 50-59.

8. VADM Jacoby, interview by author, September 2004, the Pentagon.

9. Joint Chiefs of Staff, Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: U.S. Government Printing Office [GPO], 2003).

10. Joint Warfighting Center (JWC) Pamphlet 5, *Operational Implications of the Collaborative Information Environment (CIE)* (Fort Monroe, VA: JWC, 4 June 2004), 11-12, on-line at <www.stormingmedia.us/48/4893/A489324.html>, accessed 31 October 2005. On page GL-2, the pamphlet defines the CIE as "a virtual aggregation of individuals, organizations, systems, infrastructures, and processes to create and share the data, information and knowledge needed to plan, execute, and assess joint force operations and enable a commander to make decisions better and faster than the adversary."

11. Ibid., 11-12.

12. Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World* (Cambridge, MA: Perseus Books, 1994), 440. Kelly observes that a system stuck in the present is reactive, prone to surprise from change, and will die. A common operating picture (COP) only capable of portraying real-time conditions creates digitized, myopic views of reality and cognitively handicaps anticipatory actions.

13. The specific temporal orientation is tied to resource allocation and regeneration capacity. Future and associated "times" merely show varied planning, decisionmaking, and action orientations vis-à-vis adversaries. These will vary. Joint task force commanders and national-level decisionmakers should be future-oriented in terms of weeks, months, and perhaps years. Moreover, a new field of computer science deals with anticipatory computing in dynamic environments.

14. In each example, the ability to maintain disciplined focus at the right level and dynamically integrate relevant information and understanding seamlessly with actors across all levels maintains the competitive advantage. A COP view is possible because of the enterprise information systems.

15. Martin Van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), 145. The literal interpretation of this does not convey the intent of the statement; rather, recognition of the inability to conduct detailed planning for tactical actions from higher headquarters. As Van Creveld relates: "The true essence of the Prussian command system was not to try to foresee every move in war as if it were a railway timetable."

16. BG Huba Wass de Czege and MAJ Jacob D. Biever, "Future Battle Command: Where Information Technology, Doctrine and Organization Meet," *Army Magazine* (August 2001): 10-12.

17. U.S. Army Field Manual 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: GPO, 2004), 3-13; COL Stefan Banach, discussions with author, November 2004, Fort Leavenworth, KS. Properly task-organized tactical units (mounted and dismounted maneuver, fires, intelligence, interrogation, and translation capability) with seasoned leadership and support (including pulsed sustainment, casualty evacuation, joint fires, air and ground quick-reaction forces, and robust secure communications) can conduct one tactical engagement after another (roll from target to target) to generate and continue generating exceptional information. Further empowering lower tactical levels with better organization, including the addition of unique capabilities, creates the ability to roll from target to target under an adaptive execution construct. Special operations forces with interagency support do this now. A transformed conventional force should also be fully resourced to execute operations under an adaptive execution construct.

18. JP 5-0, *Doctrine for Planning Joint Operations* (Washington, DC: GPO, 1995).

19. Partners might be U.S. Department of Defense (DOD), non-DOD, or non-U.S. coalition elements. This empowerment through decentralized data distribution requires relinquishing expert control to all stakeholders across the enterprise, to even the lowest levels, to allow adaptive planning and execution.

20. Louis Andre, Chief of Operations, Defense Intelligence Agency, interview by author, the Pentagon, September 2004.

21. If agents or actors cannot act, they cease to be agents or actors.

22. Even the most "strategic" actor or agent must take action in the tactical realm. In Operation Iraqi Freedom, the opening air strike against Saddam Hussein (at his suspected location) was still bound by the tactical, physical employment of the aircraft delivering precision munitions. Newtonian physics dominate the tactical level of war. A tactical component exists in each domain of war.

23. BG Wayne Michael Hall, *Stray Voltage: War in the Information Age* (Annapolis, MD: Naval Institute Press, 2003), 158-69. I use Hall's terminology, but U.S. Joint Forces Command (JFCOM) has similar concepts and varied terminology. JFCOM foresees the creation of distributed knowledge centers for the CIE. Knowledge centers are composed of humans, information technology, and information.

24. U.S. Army, "2003 Army Transformation Roadmap," 7-17, on-line at <www.army.mil/2003TransformationRoadmap/>, accessed 31 October 2005.

25. Cambone, 4.

26. Vision is a function of articulating the linkage between the guiding purpose and the effects-based intent. The use of specified tasks in operations orders in execu-

tion-centric, decentralized operations can inhibit initiative and create incoherence. Creating task lists from centralized planning activities is increasingly too slow and too limiting to address emerging conditions and can constrain actors from seeking and exploiting opportunities because finite resources are prioritized and committed to fulfilling prespecified tasks from "higher." These insights are from an address on U.S. Marine Corps operational planning observations during Operation Iraqi Freedom by the 1st Marine Expeditionary Force to the School of Advanced Military Studies at Fort Leavenworth, Kansas, 6 December 2004.

Tightly coupled task lists for operations resulted in continuous streams of fragmentary orders (FRAGOs) when situations changed. Many FRAGOs were irrelevant by the time they reached lower level units. In other cases, units were already engaged in the actions the FRAGO specified. Had the units waited for an order (even verbal), the action might have been too slow to produce the required effect. Because the units perceived the need to act, and did so without orders, one can question the validity, or at least the necessity, of the higher headquarters' order that followed. This places the debate about effects and tasks firmly in the "Decision Cycle Battle" forum. Task and purpose might be replaced by effect and purpose. To be sure, tasks to subordinate units or elements will not be wholly replaced, but the default behavior of specifying discreet actions to subordinates vice articulating effect-based intent might require more thoughtful investigation and doctrinal discussion.

27. The rule sets for authority to take action should clearly reflect the maximum latitude an actor has and a minimum level of control logic to accomplish the mission. Thresholds should be identified within the mission set, along with purpose and effects-based intent.

28. Purpose drives behavior. Commanders describe effects to modify and shape organizational actions to achieve an overarching purpose. Nested purpose and effects create coherence across the domains and levels of war.

29. Anonymous senior joint force commander, lecture to SAMS, Fort Leavenworth, Kansas, 2004.

30. The illusion of control exists when someone has the perception they can control dynamic and complex interactions "from the top."

31. The effects design (purpose) describes the "what" with the actors creatively determining the "how" without centralized direct control. Remember, control is maintained through indirect means.

32. JCS, *Stability Operations-Joint Operating Concept [Stability Joint Operating Concept (JOC)]* (Washington, DC, GPO, 3 October 2003), 19.

33. *Major Combat Operations (MCO)-Joint Operating Concept (JOC)*, 7. No other information given.

34. COL Leonard Wong, *Developing Adaptive Leaders: The Crucible Experience of Operation Iraqi Freedom* (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 2004), 3-6. Wong describes the complex interactions junior officers are experiencing in Iraq today. Company-level leaders and soldiers routinely interact with coalition, multiagency, and non-DOD elements as they transition daily (sometimes hourly) from humanitarian and stability support operations, to close combat operations, and back again to noncombat-related actions. Junior leaders have demonstrated remarkable adaptability, mental agility, and operational flexibility.

35. The persistent surveillance capability might determine linkages among financial transactions in Asia, the transshipment of materials in Africa, and the training of an action cell in South America. This is certain to create new methods of developing and executing operational art. We will need new mechanisms to describe, induce, and assess coherent effects. If persistent surveillance is a major contributor to generating this understanding for coherent action, it must include tailored COP as the distribution mechanism for each element taking action. The continuous Complex Adaptive System (CAS) view of the adversary creates the ability to do this.

36. Sun Tzu observed: "The highest realization of warfare is to attack the enemy's plans" (Ralph D. Sawyer, *Sun Tzu: The Art of War* [Oxford: Westview Press, 1994], 177).

37. Ralph J. Begley, Mark Reige, John Rosenblum, and Daniel Tseng, "Adding Intelligence to Medical Devices," *Medical Device and Diagnostic Industry Magazine* (March 2000), on-line at <www.devicelink.com/mddi/archive/00/03/014.html>, accessed 31 October 2005.

38. A key doctrinal component of the cavalry mission is to "gain and maintain contact" with the enemy.

39. For a definition of JOpsC, see on-line at <www.jfcom.mil/about/fact_jopsc.htm>, accessed 22 November 2005.

40. Wong. We should carefully consider how we can leverage the force that has "been through the crucible" to enhance new force and organizational capabilities. We should not squander demonstrated mental agility and capacity to handle authority with responsibility well beyond what was considered appropriate for them just a decade ago.

41. The Intelligence and Security Command Overwatch Initiative is already supporting units in combat in Afghanistan and Iraq. Division G2s and the Analytic Control Element will continue to have a purpose, but emphasis might shift from real-time support to supporting adaptive planning and effects assessment, allowing the Overwatch to provide real-time, "Knowledge Advantage Center-like" direct support to tactically engaged elements through Distributed Common Ground Systems-Army.

Major David M. Pendall, U.S. Army, is the G2 at V Corps Headquarters. He received a B.A. from Ohio University, an M.S. from Central Michigan University, and is a graduate of the U.S. Army Command and General Staff College, School of Advanced Military Studies (SAMS), Fort Leavenworth, Kansas. He has served in various command and staff positions in the continental United States, Bosnia, Korea, and Kuwait, and during Operation Iraqi Freedom in Iraq. This article is adapted from a monograph produced as a SAMS graduation requirement, and is available on-line at <www-cgsc.army.mil/carl/contendm/home.htm>.