ILW SPOTLIGHT 17-1

Army Intelligence: Focus Areas for Science and Technology

PUBLISHED BY THE INSTITUTE OF LAND WARFARE
AT THE ASSOCIATION OF THE UNITED STATES ARMY

APRIL 2017

Faced with a complex and evolving security environment, Army Intelligence requires a directional and provisional blueprint for the future. This blueprint, described in the following pages, discusses how to leverage innovative concepts and Science and Technology (S&T) to adapt to current and emerging threats while informing the design of the future Intelligence force and systems; to target and develop the right technologies to support the future force envisioned in the Army Operating Concept; and to address future long-term requirements beyond 2035. Army Intelligence must partner with industry, academia, Department of Defense initiatives, the joint community and the Army's acquisition community to develop the capabilities required to support the future force envisioned in 2025 and beyond.

In the November 1956 issue of *ARMY* magazine, Lieutenant Colonel Robert B. Rigg described the Army of 1974 as one in which Soldiers would routinely use exotic technologies such as rotor-wing aircraft, helmet radios, see-in-the-dark goggles, pocket radars and composite body armor.[1] Additionally, he foresaw an operational environment filled with "mechanical spies" and "seeing-eye drone scouts." Today, one might view his vision as quaint or dated. The Army's use of helicopters, combat vehicle crewman's helmets, night observation devices, unattended ground sensors and unmanned aircraft systems is all taken for granted. What should be appreciated, however, is the scope and breadth of his vision to project these capabilities against a future operating environment in the years immediately following the Korean War, as well as the effort necessary to bring that vision to fruition. In 1956, advances in aerospace, sensing and communications provided a glimpse into what could be. Rigg extrapolated those emerging technologies and imagined how they could be integrated into a coherent means of fighting based on his interpretation of future threats and the American way of war. If the Army is to fight and win in future wars, it must thoroughly understand the challenges that it will face and how those challenges will impact the way it intends to fight. It must act now to ensure that it possesses a technological edge over its adversaries.

The *Army Operating Concept* states that anticipating the demands of future armed conflict requires an understanding of continuities in the nature of war as well as an appreciation for changes in the character of armed conflict.

ISSUE

Army Intelligence requires a directional and provisional blueprint for the future.

SPOTLIGHT SCOPE

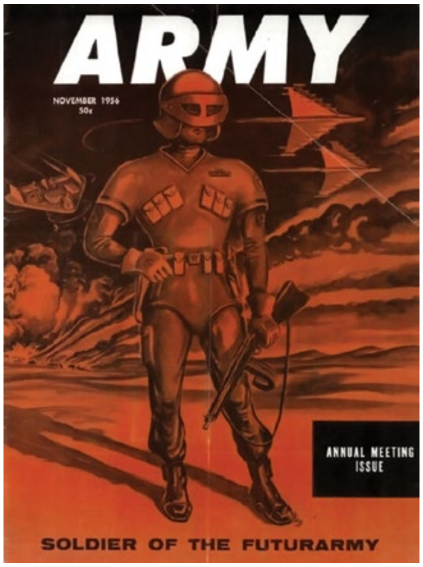
- Addresses critical Modernization efforts to close gaps in Army Warfighting Challenge #1, *"Develop Situational Understanding: how to develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations."*
- Describes how the Army will *adapt* in the near term (up to 2025), *evolve* Soldiers, systems and organizations into improved warfighting capabilities in the mid-term (2026–2035) and *innovate* dominating capabilities for the far-term (2035–2050).

IMPERATIVES

- Appreciation for changes in war's *character* (not its *nature*) due to evolutionary and revolutionary technology, evolving geopolitical stress, significant cultural changes and increasingly urban global population.
- Immediate action to secure technological edge over adversaries in the near term and in the future Operating Environment.
- Capability development to converge SIGINT, cyber, EW, human intelligence and counterintelligence.
- Partnership of Army Intelligence with national laboratories, academia and industry.

Technological advances and changes in strategic guidance, joint operating concepts and security challenges require the Army to innovate to ensure that forces are prepared to succeed in future missions.[2] This is especially true for the intelligence warfighting function, which must rapidly make sense of an increasingly complex and chaotic battlespace in an effort to reduce commander uncertainty while simultaneously **providing intelligence at the speed of mission command**.

At the same time, there are continuities in the way that the Army—and Army Intelligence by extension—will conduct operations now and in the future. It will continue to fight as part of a joint and coalition force; Army Intelligence must be interoperable with its service, joint, national and coalition partners. The ability of Army Intelligence to seamlessly exchange information and collaborate among echelons and with the intelligence community (IC) is essential to mission command,[3] particularly when addressing anti-access/area denial (A2AD) strategies that deny temporary access to intelligence assets. Achieving this end requires merging evolving Intelligence requirements with advances across the technological spectrum. As Rigg envisioned 60 years ago, Army Intelligence must continue to shape S&T efforts based on a thorough understanding of the threat and advancements in technology.



ARMY Magazine cover, November 1956.

Army Intelligence S&T Efforts in the Near Term (Now–2025): Adapting to Current and Emerging Threats

Since the 11 September 2001 terrorist attacks on the U.S. homeland, fighting domains have changed substantially. The electromagnetic spectrum (EMS) has expanded the battlespace beyond visible light and has increased the roles of space, cyberspace and electronic warfare (EW), providing enemies with new areas from which to attack and presenting a new domain to defend—cyber. Adversaries enjoy freedom of maneuver in the EMS and in social media; they can control their own messages while simultaneously denying and disrupting the messages, decisions and actions of their targets. In the same way that adversaries use dense urban areas to prevent detection and hamper application of fires, they also use the crowded Internet for command and control, essentially hiding in plain sight among millions of other users. Harnessing infra-red and other wavelengths reveals what was previously invisible. The growing range of options and battlespace afforded to them requires that the Army be prepared to fight and win across all domains while sustaining a technological advantage.

In pursuit of this technological edge, Army Intelligence is partnering with industry, academia, the services, national and service labs and partner nations to leverage ongoing technology excursions and investments. These partnerships provide opportunities to identify and understand technology trends and venture capital portfolios that inform acquisition.

Today, Army Intelligence remains engaged with a broad and diverse range of efforts. Among these are:

- the Secretary of Defense's Defense Innovation Unit Experimental and the Army's OnPoint that both aid in understanding the newest technologies coming from Silicon Valley;
- Intelligence, Surveillance and Reconnaissance (ISR) symposia and

ARMY INTELLIGENCE REMAINS ENGAGED WITH A BROAD RANGE OF EFFORTS:

- SecDef's Defense Innovation Unit Experimental;
- Army's OnPoint;
- ISR symposia and working groups;
- TRADOC's Mad Scientist Initiative;
- academic partnerships; and
- national labs.

working groups across academic and national labs including the Massachusetts Institute of Technology Lincoln Labs ISR Symposium;

- U.S. Army Training and Doctrine Command's Mad Scientist Initiative, which supports continuous dialogue among joint military partners, international partners, academia, government and private-sector organizations to help the Army explore the evolution of the Operational Environment (OE) through the year 2050. Mad Scientist also seeks to examine the effects of all aspects of technology as well as other OE factors on the future of armed conflict;
- academic partnerships with Arizona State University to study the impacts of ubiquitous social media, emerging cyber environments and evolving dense urban areas (megacities); and
- national labs, including Sandia National Labs, Lawrence Livermore National Labs and Johns Hopkins University Applied Physics Lab—as well as Army labs—which are deeply involved in supporting Quick Reaction Capability (QRC) efforts to address current and emerging threats.

These partnerships provide Army Intelligence with the opportunity to develop QRCs targeted against known gaps, such as a true multifunctional/multidiscipline mobile, survivable ground collection system to complement multifunctional teams; a means to connect ground forces with time-critical tailored biometric information; powerful analytic engines that can rapidly organize and fuse disparate bits of data into a coherent, relevant and actionable picture to relieve the cognitive burden for analysts; and a suite of mid-altitude manned and unmanned sensors capable of detecting, tracking and identifying an increasingly savvy and elusive threat.

Fielding more than 100 QRCs over the past 12 years has provided valuable insight into which capabilities and attributes work best while simultaneously informing requirements for future systems. Many QRCs remain relevant for global operations and are transitioning to existing programs of record. However, the QRC approach is limited to developing relatively mature technologies for use against known threat behaviors in specific environments. Building the capabilities required for future threats in a less certain world will entail targeting promising—but emerging and disruptive—technologies offering an edge.

Army Intelligence S&T Evolving for the Mid-term: 2026–2035

Ensuring that future Army forces are prepared to win in a complex world requires a focused, sustained and collaborative effort across the institutional Army, the operating force, the joint community, industry, academia and other partners. Army Warfighting Challenges (AWfC) provide an analytical framework to integrate efforts across warfighting functions while collaborating with key stakeholders in learning activities, modernization and future force design.[4] The U.S. Army Intelligence Center of Excellence is the lead for AWfC #1, "Develop Situational Understanding: how to develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations."[5]

The U.S. Army lives in a resource-constrained environment. Financial pressures force it to approach modernization with an emphasis on ensuring that

EXAMPLES OF CURRENT ARMY-DEVELOPED QUICK REACTION CAPABILITIES

- **Vigilant Pursuit**: Provides mobile, survivable, multi-discipline collection and processing either onsite supporting real-time exploitation or on the move supporting tactical maneuver.
- **Biometrics Identity Intelligence Repository (BI2R)**: Links enemy identities to collected information and analyzes intelligence to develop profiles used to support targeting efforts, tactical operations and force protection efforts.
- **Insight**: A Defense Advanced Research Projects Agency (DARPA) project to support data organization and analysis.
- **Medium Altitude ISR**: Multiple Aerial ISR quick reaction capabilities designed to provide specific tactical advantages or defeat enemy tactics, techniques and procedures, including:
  - wide-area surveillance, supporting pattern of life and forensic analysis;
  - light, detection and ranging (LiDAR) for greater visibility into foliage and some man-made structures;
  - vehicle and dismount exploitation radar (VaDER) to track vehicles and dismounts; and
  - Saturn Arch for advanced imaging capabilities.

the capabilities it seeks are absolutely necessary, cost-effective and fully support future Army concepts. Leveraging insights from AWfC #1, Army Intelligence marries critical emerging technologies with how the future Army force intends to fight; this allows necessary technology development to begin now, thereby enabling future capability when required. This deliberate process provides a proven, logical approach to modernization and ensures good stewardship of scarce resources. In support of the *Army Operating Concept*, Army Intelligence will pursue the following technology-based capabilities:

Laghman Province, Afghanistan. A U.S. Army Military Intelligence Soldier demonstrates how to calibrate a direction finding antenna for Afghan soldiers during the Wolfhound fielding and training. Photo by Sergeant First Class E. L. Craig.

- **Mission-tailorable, scalable and analytic tool suites for data management, integration, analysis and portable processing**: With an increase of sensors in the battlespace, the volume of available data has increased exponentially, but the pace of current and future operations will require usable, consumable, timely information and intelligence at the speed of combat. To meet that timeline and lessen the cognitive burden, future analysts will need powerful automated fusion tools capable of correlating data from various sources and enabling intricate tasks, such as activity-based intelligence analysis and identity/relationship discovery.
- **A common architecture across the modernized signal intelligence (SIGINT)/EW fleet, oriented on likely threats and contingency mission sets**: Worldwide advancements in telecommunications technologies have resulted in the need for significant shifts in technologies to intercept and exploit SIGINT information.
- **Multi-INT sensors and payloads, enabled by automated discovery and interoperability, automated processing, recognition and cross-cueing**: Even though Army Intelligence has shifted to a multifunction team organizational construct, collection devices are largely limited to one single function. Development of multi-modal sensing suites should not only correct that flaw, but also improve situational awareness by providing alternative collection to either cross-confirm or cross-cue or, at the very least, to provide some coverage when other disciplines are ineffective.
- **Collaboration and cross-domain capabilities with the IC, joint, special operations forces and coalition organizations:** Joint, interagency, intergovernmental and multinational (JIIM) interoperability efforts must conform to defined joint and international standards and technologies.
- **Advanced automated processing, exploitation and dissemination capabilities for a reduction of cognitive burden on analysts; alerting and concept extraction; entity recognition; product templating; data management; and structured observation management**: As multi-sensor collection platforms (both terrestrial and aerial) are fielded, the need to task, process, fuse, exploit and disseminate relevant observation data

ARMY INTELLIGENCE WILL PURSUE THE FOLLOWING CAPABILITIES:

- tool suites;
- common architecture across the modern SIGINT/EW fleet;
- multi-INT sensors and payloads;
- collaboration and cross-domain capabilities;
- automated processing, exploitation and dissemination capabilities; and
- capability hardening for A2AD countermeasures.

has grown more urgent. Given the volumes of such data at individual platforms (and limited bandwidth to transport it), the need exists to move initial exploitation as far "upstream" in the processing architecture as possible—even onto the platforms themselves—to optimize analyst effectiveness.

- **Systems require capability hardening for A2AD countermeasures**: On the ground-breaking edge of the Army Intelligence information technology (IT) infrastructure, units below battalion have the need for synchronized data, application and computational services just as units at higher echelons do. Transportation of relevant and locally-derived situational information from lower-echelon units into the cloud is a critical need. Development of mobile situational awareness and other relevant analytical applications that leverage enterprise data are crucial. The integrity of system development, acquisition and sustainment processes will be based on the security of individual components, incorporating the notions of "trusted sources" and "trust maintenance" to guarantee that hardware and software remain free from foreign tampering. Across every system and capability that Army Intelligence will field, tools must be tailored to meet the unique aspects of human machine interface (HMI) and human computer interface, both of which support the user experience for Intelligence Soldiers. Future tools must incorporate advances in pattern-matching algorithms, narrow Artificial Intelligence applications and automated knowledge management to provide advanced models for fusion and correlation for tailorable analytic tool suites and scalable, automated processing, exploitation and dissemination (PED) workflow and capabilities. Army Intelligence systems should allow computers to do what they are best at— number-crunching and fact-finding—so that Soldiers can do what *they* do best—analysis.

Innovating for 2035 and Beyond

Looking at the future, it is not difficult to imagine a fundamental change in the character of war. Evolutionary and revolutionary technology such as quantum computing, evolving geopolitical stress and significant cultural changes all contribute to a complex and dynamic operating environment dominated by an increasingly urban global population. The number of megacities (urban areas with more than 10 million residents) continues to increase and will challenge the ability to collect and target. These urban obstacles will be filled with various technologies that could be difficult to counter and could deny U.S. collection. New sensors must be developed that can map and understand all aspects of the urban environment, such as the utilities infrastructure. Combined, these changes in the operating environment create the potential for new technologies, novel uses of

A Soldier, assigned to the 780th Military Intelligence Brigade on Fort Meade, Maryland, sets up low level voice intercept equipment during a cyber integration exercise on Joint Base Lewis–McChord, Washington, 21 October 2015. Photo by Captain Meredith Mathis.

existing technology or a combination of the old and new technologies, all of which must be both countered and leveraged.

As threats adapt and evolve against U.S. strengths, Army Intelligence must innovate to support the Secretary of Defense's Third Offset strategy—the concept of investing in and deploying technologies in new or novel ways to meet relevant threats, thereby reducing the burden of technology overhead (maintenance, sustainment and training) for tactical forces and reducing the cognitive burden on analysts, all while filling critical operational gaps. To support these initiatives, Army Intelligence plans to leverage the new Army Rapid Capabilities Office to quickly provide new capabilities to Soldiers based on emerging threats.

Army Intelligence must innovate to support the Secretary of Defense's Third Offset Strategy.

In anticipation of these changes in the operational environment, Army Intelligence is conducting a holistic assessment of the ISR strategy from the ground up. The focus will transition to terrestrial collection platforms with increased platform survivability in A2AD environments to adapt to the shift from counterinsurgency to combined-arms maneuver.

The terrestrial layer's ISR focus is to modernize legacy ground SIGINT systems to include enhanced signal processing and increased collection range to counter rapidly evolving threats. Looking forward, capability development should converge SIGINT, cyber, EW, human intelligence (HUMINT) and counterintelligence into one system within the brigade combat team military intelligence (MI) company and corps-level expeditionary-military intelligence brigade.

While the Army completes the modernization of the aerial ISR fleet by Fiscal Year 2024, it will continue to explore both platform and sensing solutions to meet future Army and joint ISR needs against a variety of threats in potential A2AD environments. It will evaluate the proper balance of manned versus unmanned systems in all threat and weather conditions to inform decisions on what the future aerial ISR fleet should look like. The Army will also pursue sensor miniaturization to increase system performance and provide mission flexibility.

While the future cannot be predicted, current trends in technology can be examined and extrapolated to their logical ends—following the example that Lieutenant Colonel Rigg set in 1956. Advances in narrow Artificial Intelligence and machine-learning will continue to evolve, creating more powerful computer systems that can support Intelligence, both for the Army and for its adversaries. As machine-learning algorithms are refined and improved, software will be able to review super-spectral data gathered by various sensors (e.g., light, detection and ranging—LiDAR—radar, multispectral and/or hyperspectral) to determine structures and features across the entire EMS, including those invisible to the human eye. Investments in the "Internet of things"[6] and global connectivity will saturate urban environments with sensors that cover the gamut of voice, biometric, audio and social analyses, making early intelligence collection and Special Operations more challenging. Advances in robotics and machine-to-machine interfaces will create new sensing and communication platforms—but also new threat platforms. Nano-scale, biological and material sciences will produce stronger and lighter composites, presenting barriers to signature analysis and detection. Much as stealth aircraft were part of the Second Offset at the end of the Vietnam War, new materiels and collection capabilities must be

THE INTERNET OF THINGS:

The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

part of the Third Offset strategy for tomorrow.

These anticipated advancements will be available for adoption both by the U.S. Army and by its adversaries. Today's strategy is to posture capabilities that will support upgrades tomorrow. This includes investment in modular architectures—both hardware and software—that allow for plug-and-play components that are configurable and tailorable to specific mission sets.

The Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS) provides a persistent Airborne Intelligence, Surveillance and Reconnaissance (AISR) capability to detect, locate, classify, identify and track surface targets with a high degree of timeliness and accuracy during the day, night and nearly all weather conditions. It enhances Brigade Combat Team effectiveness by defining and assessing the environment and providing surveillance, targeting support and threat warning. Photo by the U.S. Army.

The Way Ahead: The Value of Partnering with Industry

To reach its future goals successfully, the Army will continue to adapt to needs or changes in the near term (up to 2025), evolve its Soldiers, systems and organizations into an improved warfighting capability in the mid-term (2026–2035) and innovate dominating capabilities for the far-term (2035–2050). Creative thinkers, subject matter experts and innovators are needed today to create a vision for both near-term advances in technology and for the future OE. The Army will accelerate closing the gap between today's Intelligence requirements and tomorrow's future force. Army Intelligence leadership values partnership with national laboratories, academia and especially industry—as is evidenced by a commitment to conduct industry days—and continually seeks ideas with a path toward innovative capability.

As the commercial sector invests heavily in data, analytics, cyber and other relevant computing and IT capabilities, the Army must leverage these investments to keep pace with technology. Doing this through and in conjunction with the acquisition community is essential, as these efforts span both the commercial and academic sectors.

Looking beyond the near term, Army Intelligence must invest in more survivable autonomous collaborative operations via unmanned platforms, including the potential use of swarms, manned-unmanned teaming and collaborative autonomous systems as a means to defeat adversaries. These new platforms will require modernization of sensing and processing suites to accommodate changes in methods of data collection. Smarter sensors should provide processing and initial fusion at the point of collection, allowing for optimized use of network bandwidth and faster, more pertinent information about an area of interest. Advanced HMI for collection, analysis and synchronization will require improved visualization, conceptualization and interaction of users with situational data in both time and space; advanced techniques for improved human interaction with large volumes of data; rapid advancement of market HMI capabilities into Army MI systems; and immersive training approaches. Army Intelligence will also explore and develop technologies to reduce the burden imposed by the vastness of available sensor data on the analytic force. Finally, Army Intelligence will be much more involved in EW and the management of its

As the commercial sector invests heavily in data, analytics, cyber and other relevant computing and IT capabilities, the Army must leverage these investments to keep pace with technology.

own signatures. The skills of the MI community are exactly the skills required to understand and manage the radio frequency, electro-optic/infra-red and social media signatures of the Army's own forces and to assess their impact.

Just as Rigg did in 1956, today Army Intelligence looks toward future evolutions and revolutions in technologies that will be available both to it and to its adversaries. Making the best use of taxpayer dollars, its approach is deliberate and focused, identifying solutions to the most critical challenges. Relying on academic and commercial partners, Army Intelligence is well-positioned to develop and acquire the innovative technologies needed to provide intelligence to the future Army force at the speed of mission command.

Vigilant Pursuit provides dedicated tactical pursuit vehicle-mounted and dismounted assets that employ cutting-edge technologies, enabling signals- and human-intelligence Soldiers to cross-tip and cross-cue timely intelligence to more rapidly and accurately identify high-value targets. Photo by Kashia Simmons.

[1] Lieutenant Colonel Robert B. Rigg, "Soldier of the Future Army," *ARMY Magazine*, (November 1956), pp. 24–37, https://www.ausa.org/publications/soldier-futurarmy.

[2] Department of the Army, *The U.S. Army Operating Concept: Win a Complex World*, TRADOC Pamphlet 525-3-1, 31 October 2014, pp. 8–15, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

[3] Army Doctrinal Publication 6-0, *Mission Command* (Washington, DC: Government Printing Office, May 2012), p.1. Mission command is defined as "the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations."

[4] Department of the Army, *The U.S. Army Operating Concept: Win a Complex World*, TRADOC Pamphlet 525-3-1, 31 October 2014, p. 31, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

[5] *Ibid.*

[6] The *Oxford English Living Dictionary* defines the "Internet of Things" as "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."

The Association of the United States Army is a private, non-profit educational organization that supports America's Army—Regular Army, Army National Guard, Army Reserve, retired Soldiers, government civilians, wounded warriors, veterans, concerned citizens and family members.

Interested in becoming a member of AUSA? See the benefits of membership and join online at:

www.ausa.org/membership