The Transformation of Army Intelligence

by Lieutenant General Robert W. Noonan, Jr.

Emerging world trends point to a period of unbounded strategic challenges, a wider range of threats, increased unpredictability, and a more complex range of operating environments that will challenge the United States at every level of intensity. Our country will require a world-class Army capable of rapid response and dominance across the entire spectrum of operations. A broad range of well-balanced, responsive land force capabilities, employed within a joint operational framework, will be critical to sustain land dominance. To meet this demand, the Army is transforming along three major, concurrent axes: Trained and Ready, Transforming the Operational Force, and Transforming the Institutional Army. This article provides some perspectives on the implications of Army transformation for the Military Intelligence Corps (see Figure 1).

Army Intelligence Transformation

The goal of Army Intelligence is to achieve situational dominance for Army decision-makers and warfighters. Key to this is information superiority that enables the seven operational characteristics of the Army Objective Force: responsiveness, deployability, agility, versatility, lethality, survivability, and sustainability. Situation-dominating results give commanders the ability to acquire, track, engage, and assess targets, thus dominating the battlefield environments and situations across the spectrum of conflict. Army Intelligence is already moving out on the path to achieve this. We are developing and employing a seamless architecture that provides an enhanced situational awareness through internetted command, control, communications, and computers (C^4), and intelligence, surveillance, and reconnaissance (ISR) platforms. These platforms provide commanders with a common view of the battlefield across all echelons while leveraging the capabilities of higher echelons through reach-back capabilities.

As the Army builds from the Initial to the Objective Force, Army Intelligence will apply lessons learned, incorporate available technology, and make essential changes in training and doctrine to ensure seamless support (see Figure 2) while accelerating investment and experimentation with new technologies that support Objective Force requirements. The Intelligence Objective Force will be capable of providing enhanced situational understanding, battlespace visualization, and information superiority through collaborative, interactive, integrated, and interoperable intelligence databases and networks. Army Intelligence achieves significant efficiencies operating within the Global Information Grid. Improved simulations will train intelligence soldiers anywhere, and collaborative analytical tools will give them access to regional and technical expertise anytime.

Regardless of changes, the fundamentals will remain true – Intelligence must allow warfighters to:

- Gain greater situational awareness
- Shape the battlefield
- Attain dominant maneuver and precision fires

- ❖ Reach-back
- ❖ Greater interoperability/Jointness
- ❖ Embedded ISR
- ❖ Restructured ASCC/theater support
- ❖ Restructured SIGINT
- ❖ Focus on CI/HUMINT (SSC)
- ❖ Pooling of linguist support

See the glossary on page 64 for expansion of the acronyms.

Figure 1. Transformation Changes in Military Intelligence.

Enabling Transformation through S&T Investment and Technology Protection

ISR Modernization. As the Army begins to shape its future forces and capabilities under the Transformation Campaign Plan, advanced

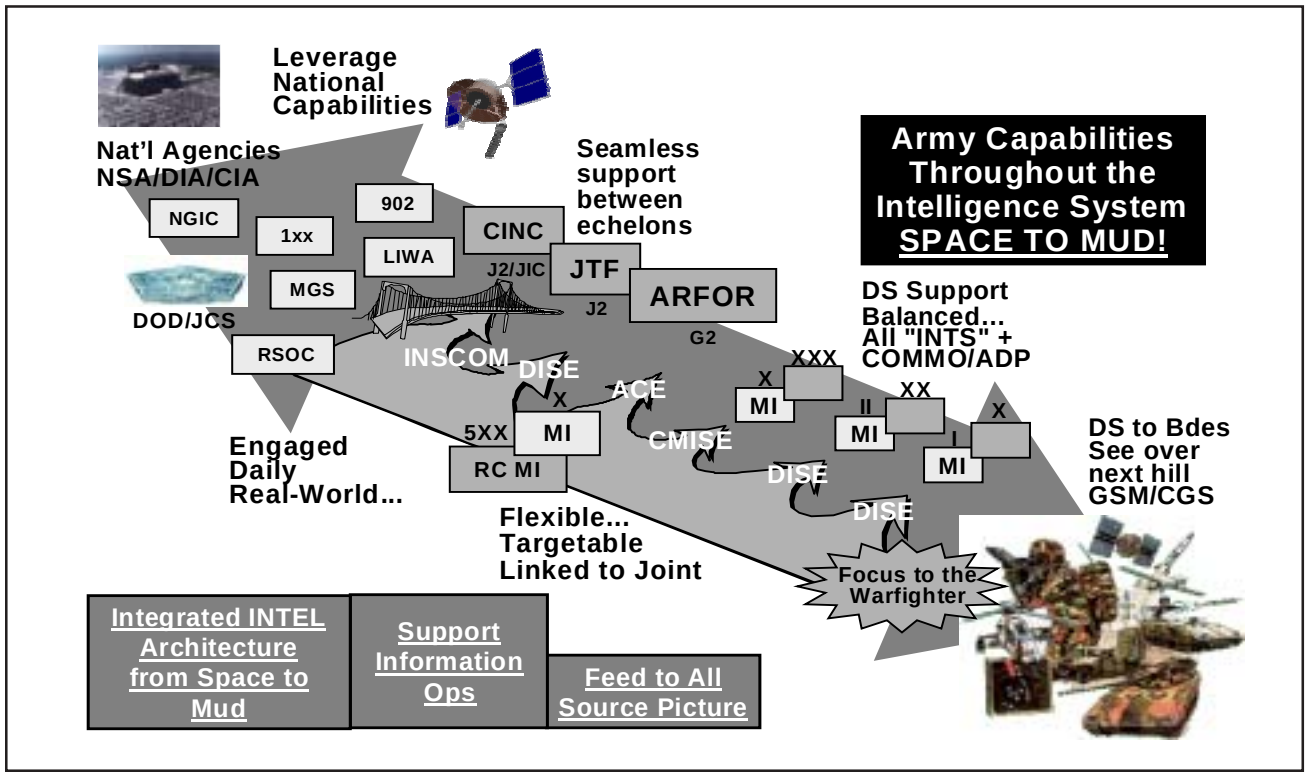

Figure 2. Army Seamless Support.

technology will serve as the crucial enabler for both achieving and maintaining combat overmatch for Army elements engaged against any adversary. Army ISR initiatives (see Figure 3) focus on migrating to fewer, but more capable, multidiscipline platforms with modular sensors, integrated processors and preprocessors, and global information access through the tactical info-sphere. Introduction of new technology will allow rapid analysis, production, and dissemination of intelligence to ensure a common operational picture on a dispersed battlefield.

Future Tactical Unmanned Aerial Vehicle (TUAV) payload upgrades will continue the trend toward a multidiscipline ISR approach. We will maximize the value-added potential of tactical signals intelligence (SIGINT) systems by transitioning measurement and signature intelligence (MASINT) capabilities from its scientific and technical (S&T) focus to operational and tactical intelligence applications in support of warfighters. Advanced technology also enables us to merge Airborne Reconnaissance Low (ARL) and Guardrail Common Sensor (GRCS) into a single airborne platform, Aerial Common Sensor (ACS), improving the commander's view of the battlefield despite diverse weather, foliage, and low-light conditions. Similarly, our numerous TENCAP (Tactical Exploitation of National Capabilities) systems will eventually integrate into a single system, the Distributed

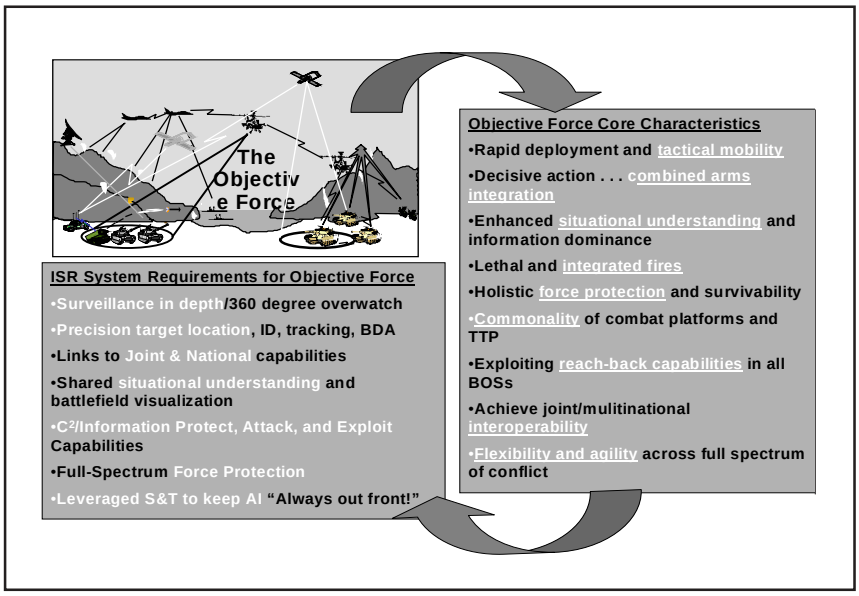

Figure 3. ISR Support to the Objective Force.

Common Ground System–Army (DCGS-A). DCGS-A will provide a multidiscipline, interoperable, common, open systems ISR and targeting architecture, and critical sensor-to-shooter links. Additionally, Army Intelligence continues to develop a computer network exploitation capability supporting both computer network attack and defense.

Avoiding Technological Surprise. With the need to exploit technology to shape future ISR capabilities comes the requirement to prevent that same technology from falling into the hands of potential adversaries. Traditionally, our technology-protection methodology centers around two axes: first, controlling the distribution and flow of technical information while securing Army laboratories and second, monitoring adversaries' access to advanced technology and reporting on their capabilities to develop battlefield abilities that threaten U.S. interests and military forces.

Maintaining the Army's technological edge in the future will demand a new, holistic approach to technology protection. This approach will continue to rely on traditional measures, but will also demand greater attention to adversary attempts to thwart U.S. technological superiority through denial, deception, and asymmetric means. Furthermore, we will have to focus significantly more attention on the exponential growth in technology itself, which—combined with the often cumbersome military research and development (R&D) and procurement processes—could result in military capabilities that are technologically obsolete within a few years of initial deployment. Finally, accompanying the challenges of traditional foreign disclosure programs will be the difficult task of managing the disclosure of advanced technology to allies and industry alike.

The Chief of Staff of the Army (CSA) has charged the Army staff, with DA DCSINT (Deputy Chief of Staff for Intelligence) lead, to assess our current technology-protection strategy and to ensure that the Army is properly focusing on the critical technologies essential to achieving Objective Force R&D, acquisition, and procurement milestones. Crucial to success is our ability to synchronize the technology-protection programs and priorities across a variety of Army agencies and staffs. We must also assess our foreign disclosure programs to ensure that we maintain the right balance between the competing objectives of foreign military sales and technology protection. The realities of the global economy, and the technological and information revolutions that underpin it, will require great flexibility in Service and Department of Defense foreign disclosure policies. In spite of all this, the bottom line remains clear. The Army must ensure it maintains a combat overmatch capability against all potential adversaries.

Conclusion

In the future, the U.S. Army is likely to face adaptive enemies using advanced technology to attack us in asymmetric ways in increasingly complex situations and terrain. To ensure success, Army intelligence must provide ground commanders with—

- "360 degree" surveillance.
- Precision target identification, tracking, and battle damage assessment (BDA).
- Internetted tactical communications and intelligence links that facilitate continuous access to joint and national capabilities.
- Support to command and control (C^2) and information-protect, -attack, and -exploit, and full-spectrum force protection.

Army Intelligence recognizes the challenge posed by the changing nature of warfare. We are actively improving current capabilities to meet the evolving needs of today's National Military Strategy while simultaneously developing new capabilities to meet the requirements of Joint Vision 2020 and the Army's Transformation Plan.✹

Lieutenant General Noonan became the DA Deputy Chief of Staff for Intelligence (DCSINT) 17 July 2000. Commissioned through the Reserve Officers Training Program, his initial assignment following graduation from the Infantry and Military Intelligence Officer Basic Courses was as a IV Corps intelligence and operations advisor in Vietnam. His other staff positions include Brigade S2, 1st Brigade, 3d Infantry Division (ID); Plans Officer and Manpower Management Analyst at Fort Devens, Massachusetts; Division Artillery S2 and Deputy Division G2, 25th Infantry Division, Schofield Barracks, Hawaii; Tactical Intelligence Officer, Rapid Deployment Joint Task Force and U.S. Central Command (CENTCOM); G2, 25th ID (Light), Schofield Barracks; Deputy Chief and Division Chief, Intelligence and Electronic Warfare/Command and Control Countermeasures, DA, Deputy Chief of Staff for Operations (DCSOPS); Executive Officer to the DA DCSINT; DA DCSOPS, U.S. Army Intelligence and Security Command (INSCOM); and the Director for Intelligence, J2, CENTCOM. LTG Noonan's command assignments include company command at Fort Campbell, Kentucky, Fort Devens, and Schofield Barracks; Commander, 125th MI Battalion; Commander, 513th MI Brigade; and Commanding General, INSCOM. His military schooling includes the Armed Forces Staff College and the U.S. Army War College. LTG Noonan earned a Bachelor of Arts degree in Government and International Relations from the University of Notre Dame and a Master of Business Administration degree from Western New England College. For more information, readers can contact COL Samborowski via E-mail at Leonard. Samborowski @hqda.army. mil.