ARMY MULTI-DOMAIN INTELLIGENCE

# FY21-22 S&T Focus Areas

Department of the Army
Office of the Deputy Chief of Staff, G-2

1000 Army Pentagon
Washington, DC 20310-1000

v1.0 - 13 October 2020

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 ARMY PENTAGON
WASHINGTON, DC, 20310-100

HQDA DCS G-2
Intelligence Surveillance and Reconnaissance Task Force

Fiscal Year 2021-2022

# Multi-Domain Intelligence Science and Technology Focus Areas

**Background.**

The Army G-2 and Army Intelligence, Surveillance, and Reconnaissance Task Force (ISR TF) maintains this living characterization of Science and Technology (S&T) focus areas critical to the ability of Army Intelligence to counter tactical, operational, and strategic threats. These focus areas support the two lines of effort, Counterintelligence Reform and Modernization, outlined in The Army Intelligence Plan (TAIP), however, unlike the non-adaptive approaches by which the Big 5 were created in the 1970s, today's military intelligence modernization must achieve these objectives through rapid prototyping and a bias towards common hardware and software solutions that can be tailored to mission and user needs, coupled with a secure supply chain, a trusted workforce, and an empowered, trained user community.

Periodically updating and publishing these focus areas:

(a) Enables Army Intelligence to stay ahead of the continuously evolving threat.

(b) Provides an understanding of Army Intelligence needs to the broader Army S&T ecosystem, industry, academia, and other government agencies.

(c) Provides a mechanism for Army Intelligence to continuously dialogue with industry, academia, and government agencies as needs evolve.

**Army Intelligence systems must be:**

1) Tailored to provide timely value to decision makers against the specific tasks for which they are employed;
2) Protected from adversary theft attempts of intellectual property;
3) Interoperable and integrated with Army command and control (C2) systems;
4) Tailorable based on mission need;
5) Interoperable with Joint, Special Operations, Mission Command, C2, and Unified Action Partners;
6) Easy to learn and sustain;
7) Continuously updating and delivering value to support the mission.

# ARMY MODERNIZATION PRIORITIES

| | |
|---|---|
| 1 LRPF<br>LONG RANGE PRECISION FIRES | LRPF CFT |
| 2 NGCV<br>NEXT GEN COMBAT VEHICLES | NGCV CFT |
| 3 FVL<br>FUTURE VERTICAL LIFT | FVL CFT |
| 4 NETWORK/C3I | NETWORK CFT<br>ASSURED PNT |
| 5 AMD<br>AIR & MISSILE DEFENSE | AMD CFT |
| 6 SOLDIER LETHALITY | LETHALITY CFT<br>STE CFT |

The Secretary of the Army and the Chief of Staff of the Army established eight Modernization Cross-Functional Teams (CFT) aligned to the six Army Modernization Priorities and two Task Forces (TF). Modernization efforts, by, with, and through Army Futures Command (AFC), guide S&T efforts, long term investments, and capability development. These Modernization-aligned CFTs are:

(a) Long Range Precision Fires

(b) Next Generation Combat Vehicle

(c) Future Vertical Lift

(d) Network

(e) Assured Positioning, Navigation, and Timing

(f) Air and Missile Defense

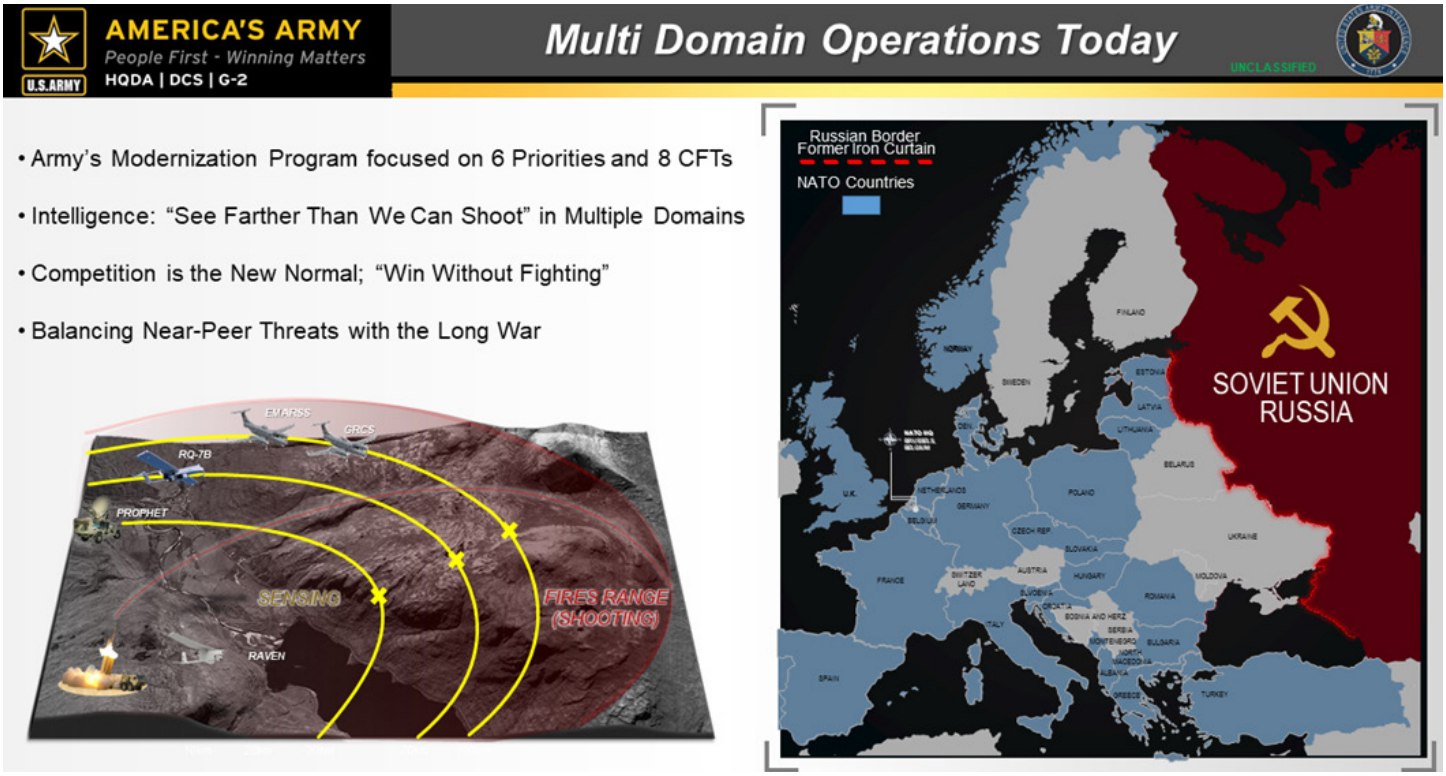
(g) Soldier Lethality

(h) Synthetic Training Environment

The two TFs within the Army supporting modernization are:

(a) Artificial Intelligence (AI)

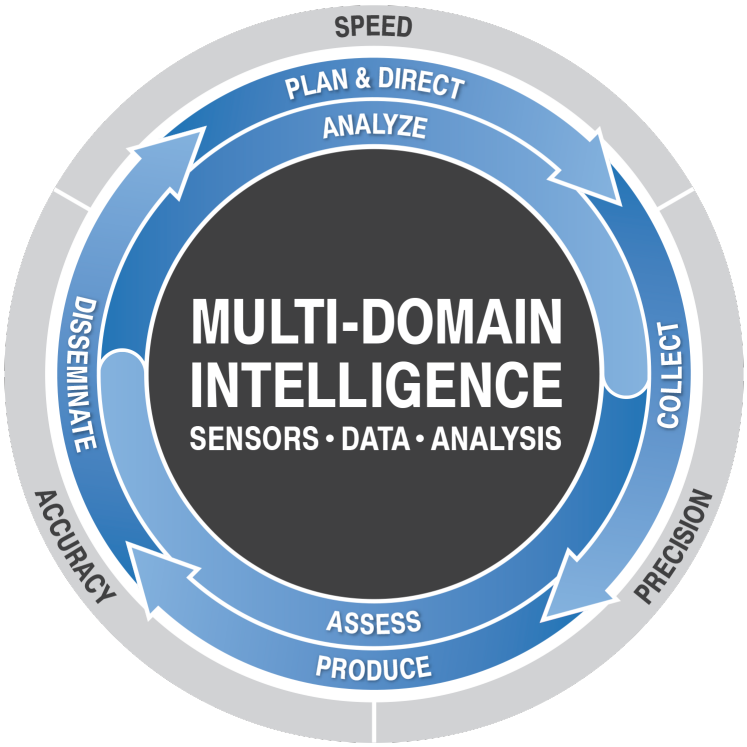
(b) Intelligence, Surveillance, and Reconnaissance (ISR)




The 2018 National Defense Strategy (NDS) highlights our need to address a return to strategic and great power competition with China and Russia, to face rogue nations such as North Korea and Iran, and to consolidate gains made in the Middle East. To achieve these ends, Army Intel must balance risk with modernization across a non-linear battlefield while embracing technology ideas and solutions. We must better leverage private sector research and development investments, while aggressively partnering with the Intelligence Community (IC) and the Joint Force.

The Army Intelligence Enterprise (AIE) must lean forward to support Army modernization by embracing new technologies, new approaches, and new ideas, in the near, mid, and far terms. The Army fights as part of the broader Joint All Domain Command and Control (JADC2) enterprise, integrated with Coalition and Partner Nation forces who bring a unique mix of capabilities that the Army will have to leverage in complex environments. Given the guidance from the NDS and the Army's Multi-Domain Operation's (MDO) strategy to address Strategic Competition, Army Intelligence must be agile and flexible with information sharing, leveraging technology to implement digital policies for information sharing with Coalition Partners and Allies across Coalition and U.S. Only networks. Layered standoff for MDO will require layered and collaborative sensing, and synchronization between C2 and Intelligence to enable persistent situational understanding. This intelligence convergence includes architecture, configuration control, management, and policy enforcement. Intelligence convergence is critical to gain, maintain, and sustain our competitive edge against adversaries and more efficiently bring effects to bear, support the rapid integration of all domains of warfare, and dis-integrate enemy capabilities to open windows of opportunity in Anti-Access/Area Denial (A2AD) environments. The ISR TF, established in conjunction with the AFC Sensing Integrated Product Team (IPT), is the Army's lead for modernization of ISR capabilities across the Space, Aerial, Terrestrial, and Foundational layers. These modernized capabilities will necessarily inform and depend on a robust foundation layer of the people, processes, and technology providing data and data services across a range of information technology services supporting the AIE.

The 2019 Army Intelligence Plan (TAIP) establishes the vision to "Deliver a Ready, Total Army Intelligence Team to Enable Multi-Domain Operations by 2028 and Dominate by 2035." The modernization framework, Multi-Domain Intelligence (MDI), coupled with a modernized Counterintelligence and security enterprise, achieves this vision. MDI aims to increase the speed, precision, and accuracy of the intelligence cycle while fully integrating Intelligence, Mission Command, and Command and Control (C2). The three pillars of MDI are: Sensors, Data, and Analytics.




Industry continues to lower the barrier to entry for advanced technology adoption. State and non-state actors are able to operationalize new capabilities with minimal investment – bringing new capabilities to parity with currently fielded systems. Wars will be fought at hyper speed and scale, dominated by technologies such as robotics and autonomous systems (RAS), machine learning (ML), and AI capabilities, which are widely available, packaged, and ready for use. The Internet of Things (IoT), connected by 5G and beyond networks, will further democratize sensing and data, enabling collaborative sensing. Investments in mapping and localization services and self-driving vehicles will bring once niche sensing phenomenologies such as light detection and ranging, radar, and multispectral sensing to a wider audience. Militarization of dual-use technology will continue to be a challenge to which the intelligence enterprise must be able to provide traditional and non-traditional indications and warning, analysis, targeting, and force protection functions.

**Army Intelligence Science, Technology, and Innovation Focus Areas for Fiscal Years 2021-2022:**

Partnerships are increasingly important to establish and maintain in order to leverage investments in capabilities that have shared applicability. While working with the Marine Corps, Air Force, Navy, Space Force, Coast Guard, Special Operations, our Coalition allies, and non-US partners, and Intelligence Community partners, Army Intelligence will share capabilities across the areas of:

(1) Counterintelligence and Technology Protection.

(2) Cross Security and Classification Domain data sharing with Joint and Allied partners.

(3) Governance and common services such as Application Programming Interfaces (API), common data foundations, and common interfaces.

(4) Machine Intelligence and enablers such as cloud technologies, development security and operations (DevSecOps), and data labeling.

(5) Increasing compute efficiency, scaling, and reducing Size, Weight, and Power (SWaP) while increasing resolution of our sensors and communications.

(6) Modeling and Simulation (M&S) to support AI-enabled wargaming.

(7) Reducing cognitive burden on Analysts and increasing cognitive dominance.

(8) Leveraging Publicly Available Information (PAI), Open Source Intelligence (OSINT), and non-traditional information.

(9) Improving the range and access for capabilities in GEOINT, Electronic Warfare (EW)/

Signals Intelligence (SIGINT)/Identity Intelligence systems based on adversary signals of interest (SOI) and activities.

(10) Countering threats from unmanned systems – space, air, ground, and otherwise.

(11) Collaborative and distributed: sensing, effects, and mission management.

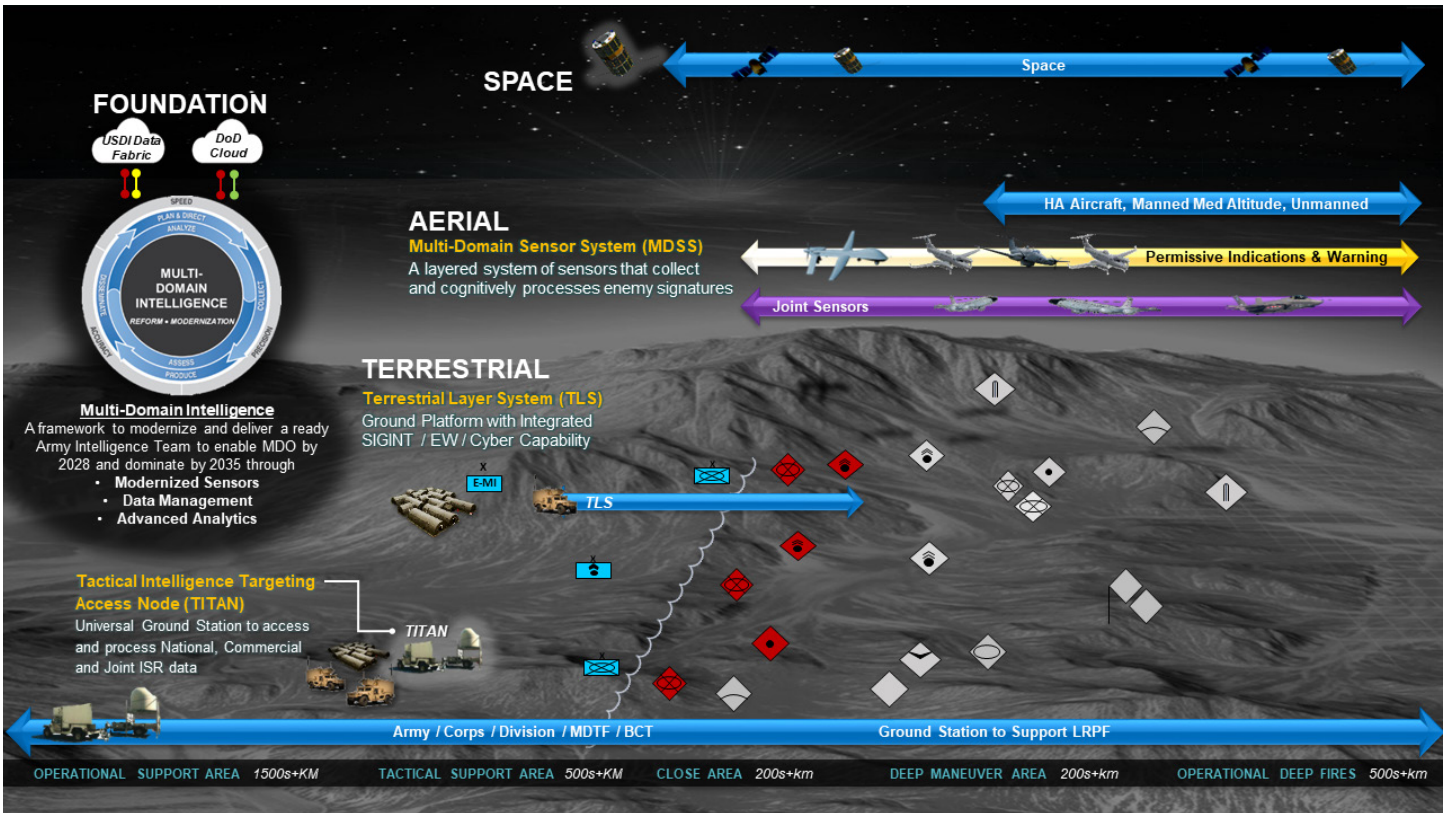
Given these conditions, the FY 2021-2022 MDI S&T focus areas are:

## SENSORS

**Sensors** – All-Domain, Collaborative, AI-Ready, and Instrumented: The ISR TF seeks deep sensing and expeditionary ground station technologies for rapid prototyping. Future sensing must consider counter-sensing and military deception in the design and deployment. Desired characteristics for future sensing capabilities are:

(a) All-Domain Sensing: Increased persistence, standoff range, and frequency range of GEOINT, RF, and Identify Intelligence systems. Increased dynamic range, further focal plane development, and increased collection distances to target at long range. Sensors capable of operating at extended ranges and providing automated target recognition for Long Range Precision Fires and Indirect Fires. Automated and dynamic sensing orchestration to collect and characterize both threat and environmental signatures to support all aspects of Army operations including deep, urban, and subterranean domains. Emerging technology to leverage traditionally manned aircraft as optionally or remotely piloted platforms to achieve sensor penetration in A2AD environments. Integrated Cyber/SIGINT/EW systems to enable use of the network as a weapon system. Novel combinations of sensors and robotic platforms that can not only move across terrain, but maneuver to sense.

(b) Collaborative Sensing: Layered sensing leveraging Space Force, Space Development Agency, Army, Joint Service, and Intelligence Community capabilities to counter an adversary's layered defense, collaborative and distributed sensing orchestration across intelligence and non-intelligence sensors, as well as collaborative and distributed effects delivery.



(c) AI-Ready Sensing: Sensing with onboard processing for characterization at the point of collection; Open Architecture Sensor Integration capabilities to support rapid integration of sensor data, dynamic discovery, automated collaborative collection, automated collaborative tasking; and a Command and Control sensor web that allows for control of sensors across the battlespace enabling automated cross-cueing and automated tracking. Automated exploitation of and Automatic Target Recognition (ATR) of peer/near peer threats across multiple phenomenologies (e.g. RADAR, SIGINT, EW/Cyber, Optical sensing, and Magnetics) trending towards areas such as quantum and gravimetry.

(d) Instrumented Sensors: Sensors prototyped and leveraged by the Army should provide instrumentation necessary to leverage Internet of Things technologies. Instrumented sensors provide constant feedback to tele-operations and local, edge, and robotics processing.

## DATA

**Data** – Governed, Discoverable, Accessible, Sharable: Data Centricity and Signature Management are critical to Combined JADC2 and MDO. Predictive analytics require clean and annotated data. Multi-Domain Command and Control requires continuous integration, shared situational understanding, and consistent capabilities across Mission Command at the data level, regardless of how capabilities are deployed. Diverse data types and schemas from sources across multiple domains require rapid aggregation. Data must be safeguarded against malicious and unintentional alteration and analysts need the capability to automatically evaluate data provenance while not limiting machine-to-machine wire-speed access to data. Data to support this end-state in large scale combat operations exists across a variety of media (e.g. hard drives, well formatted data sources, pdfs, PowerPoints, foreign articles, multi-language data repositories, pictures, videos, etc.). To achieve this the desired characteristics and capabilities are:

(a) Governed Data for Security and Management: Data governance tools to adhere to proven standards for security and interoperability to remain technology agnostic; Distributed Ledgers and execution of digital smart contracts for managing data pedigree and updates through distributed handling and processing including cross-domain data handling and multi-national data sharing.

(b) Discoverable Data Across Systems: Automatic data extraction from non-traditional sources such as manuals, literature, and PAI.

(c) Accessible Data Usable by All: Modular data transformation and automated ingestion tools that can also be used to quickly generate statistical models for analysis; capabilities that can fuse or stitch ontologies, schema, and knowledge graphs of multiple datasets and model the relationships between them.

(d) Shareable Data Produced Across Systems: Libraries of annotated multi-int training data from multiple view angles (ground-to-ground, ground-to-air, air-to-air, air-to-ground) to train machine-learning algorithms. Fusion of data about a specific object co-located in time and space: there is still an unmet need for broader fusion of dissimilar sensor phenomenologies and modalities to support MDO.

## ANALYSIS

**Analysis** – Sharable, Technology Augmented, Mission-Tailorable , and Edge-Ready: The Automation of analysis is the key to increasing efficiency and effectiveness of analysts. Industry has adopted various methods to speed the process of delivering useful capability and value to users. This focus on value drives the need for agile capability development and DevSecOps for continuous delivery and integration of new capabilities based on direct user demand. The desirable characteristics for analytic capabilities include:

(a) Shareable Analytics and Services: Micro-service based Machine Learning Operations compliant tools and models for transfer learning; automated support to the Intelligence Preparation of the Battlefield (IPB) process as part of the Military Decision-Making Process.

(b) Technology Augmented to Reduce Cognitive Burden: Army G-2 is interested in tools and automated workflows to Conduct Intelligence PED missions and tasks supporting warfighters in three primary ways: Expeditionary PED operations, Cloud enabled Reach PED operations, and PED Readiness Training. The Army needs capabilities for identifying friendly and adversarial Information Maneuver operations.

(c) Mission Tailorable Support to IPB: Automated Course of Action analysis, dynamic collection orchestration, activity and knowledge modeling, automated effects recommendations based on the environment and available capabilities across the Intelligence and non-Intelligence Joint and Coalition Forces, and automated physical and functional combat assessment to continuously feed the IPB process. Reduction of cognitive burden through technology-augmented analysis, Robotic Process Automation (RPA), automated semantic extraction, and automated Order of Battle Analysis; these solutions should be flexible enough to deploy on-premises at the government's discretion or as a cloud offering, tailorable to refine Situational Understanding – particularly in Disconnected, Intermittent, Low bandwidth (DIL) environments.

(d) Edge Ready Intelligence Support to Operations: Able to maintain coherence with the broader enterprise to prevent suffering from data drift; able to expedite the passing of target data to Army and Joint firing systems through automation and rapid synthesis of target data directly from sensors to pre-trained edge machine intelligence models.

## FUTURE OF THE ENTERPRISE AND ENABLERS

**Future of the Enterprise and Enablers** – Security, Foundations, and Training: During overseas contingency operations in the Middle East, the Army enjoyed ample bandwidth to enable reach operations for the majority of PED processes. The potential for Large Scale Combat Operations (LSCO) has called our proverbial bluff on investment, driving the need to invest in robust hybrid-cloud enabled capabilities, but also capabilities that can operate in a DIL communications environment. Whereas previously the operational need for quick reaction capabilities resulted in turnkey, stove piped software solutions, now, the Army G-2 and Army Intelligence team will leverage Department of Defense (DoD) approved "best-of-breed" common development tools and services to enable rapid implementation of new analytics. To achieve this, Army Intelligence will require:

(a) Security to Protect Intelligence Modernization: Counterintelligence and protection of intellectual property from adversary attempts at theft and compromise. Capabilities to support software and hardware supply chain transparency

to identify and track the provenance of all imported software, and determine required security procedures.

(b) Foundations to Build on: The Army Military Intelligence (MI) Commercial Cloud Service Provider is the de-facto governance and tenant pipeline for Army MI Commercial Cloud, while the DoD establishes the DoD Cloud Initiative and the Intelligence Community continues to expand the Intelligence Community Commercial Cloud Enterprise. Shifting towards a culture of DevSecOps and automated security and risk management, the Army G-2 is interested in enabling technologies for ML, AI, RPA, and Data Science, including validated and analysis-ready labeled data and leveraging existing, tailorable, models. Leveraging these foundational infrastructure service providers and system on a chip to provide edge processing and host analytics on the move. This includes leveraging commercial and government investments in massively scalable compute such as Exascale compute projects.

(c) Training the Future MI Force: Enabling Technologies also include capabilities to train and upskill our force in the development, deployment, and trust of AI and robotic systems. Employing these advanced technologies requires that Intelligence professionals have the skills and training aids necessary to articulate requirements, deploy new capabilities, train algorithms, refine collection parameters, assess effectiveness, and operate these capabilities in complex operating environments. The ability to conduct realistic training, and training that adapts based on the skills of the user, depends on the ability to accurately and completely characterize the operating environment.

---

The Army G-2 will champion necessary enabling technologies such as increased understanding of cognitive performance, increased efficiency in computing, and deployment of new computing architectures such as tensor processing, neuromorphic processing, and cognitive radio capabilities. The intent is to leverage emerging technologies, provide revolutionary concepts of operation, and accelerate intelligence capability modernization in support of the National-to-Tactical Intelligence Enterprise.

Industry, academia, and government partners can reach out to the Army G-2 Future Capabilities and Innovation Team at: **usarmy.pentagon.hqda-dcs-g-2.list.sci-tech@mail.mil**.

IN COLLABORATION WITH:

U.S. Assistant Secretary of the Army for Acquisition, Logistics, and Technology

Program Executive Office, Command, Control, and Communications (Tactical)

Program Executive Office, Intelligence, Electronic Warfare and Sensors

Office of the Deputy Assistant Secretary of the Army for Research and Technology

HQDA ISR TF

U.S. Army Training and Doctrine Command

Cyber Capability Development Integration Directorate

Aviation Capability Development Integration Directorate

Cyber Capability Development Integration Directorate

Fires Capability Development Integration Directorate

Intelligence Capability Development Integration Directorate

U.S. Army Futures Command

U.S. Army Futures Command, Army Applications Lab

U.S. Army Futures Command, Al Task Force

U.S. Army Futures Command, Sensing IPT

U.S. Army Futures Command, OSI

U.S. Army Futures Command, LRPF CFT

U.S. Army Futures Command, NGCV CFT

U.S. Army Futures Command, FVL CFT

U.S. Army Futures Command, AMD CFT

U.S. Army Futures Command, A/PNT CFT

U.S. Army Futures Command, SL CFT

U.S. Army Futures Command, STE CFT

U.S. Army Futures Command, N CFT

U.S. Army Futures Command, FCC

U.S. Army Combat Capabilities Development Command

U.S. Army Combat Capabilities Development Command, ARL

U.S. Army Combat Capabilities Development Command, C5ISR Center

U.S. Army Engineer Research and Development Center

U.S. Army Space and Missile Defense Command

U.S. Army Special Operations Command

Office of the Under Secretary of Defense for Intelligence and Security