APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

2024 ARLIS ANNUAL REPORT

TABLE OF CONTENTS

Letter from the Executive Director 2

A Strategic Asset for National Intelligence & Security 3-4

Core Capabilities 5-8

Mission Imperatives 9-12

Implementing Intelligence Insights 13-20

Growing the Pipeline 21-22

Cultivating Collaboration 23-24

ARLIS Financial Overview 25

Working with ARLIS 26

LETTER FROM THE EXECUTIVE DIRECTOR

As the new Executive Director of the Applied Research Laboratory for Intelligence and Security (ARLIS), I am excited to share our Annual Report, which highlights our progress and future directions we are charting. Since our establishment in 2018, ARLIS has become a key asset for the Department of Defense (DoD) and the national security community. This year has been one of achievement, marked by groundbreaking contracts, innovative research initiatives, and an expanded focus on critical mission areas like cognitive security and supply chain security and transformative technologies like artificial intelligence (AI) and quantum.

As I step into my new role, I'm committed to not only strengthening and advancing our core research capabilities but also to fostering greater collaboration with academic institutions, private industry, and government partners. By aligning our efforts with the needs of our partners, we will create an innovative ecosystem, ensuring that all those involved feel valued, supported, and excited about the shared mission ahead.

Our work continues to evolve as we address the growing demand for more integrated, multidisciplinary approaches to security. We are pushing the boundaries of human-machine teaming, exploring the ethical implications of AI, conducting vital research into asymmetric warfare and insider threats, and exploring how governments can best secure critical supply chains. We are leveraging quantum technologies to ensure that the United States remains at the forefront of this emerging field, and we are expanding our capabilities to improve operational readiness through human performance research and cognitive security.

As the strategic environment grows in complexity, ARLIS's cutting-edge research and development is becoming more critical than ever. Looking ahead, we will continue to deliver the intelligence insights, technological innovation, and research solutions needed to meet the challenges of a rapidly changing world. Our commitment to excellence, adaptability, and collaboration is firm, and we are eager to continue building on our strong foundation to support our nation's security priorities.

Thank you for exploring our achievements and initiatives in this report. As we look to the future, I am confident that ARLIS will remain an important partner in advancing national security through its transformative technologies and the visionary leadership of its researchers.

Dr. John Beieler
ARLIS Executive Director

A STRATEGIC ASSET FOR NATIONAL INTELLIGENCE & SECURITY

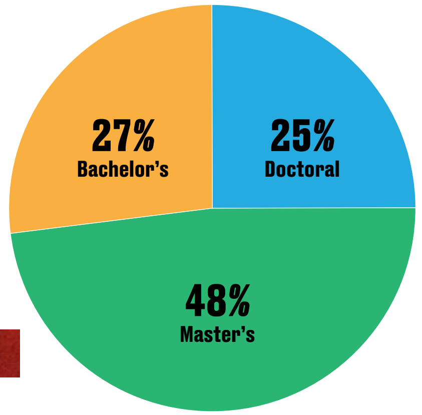
Since its establishment in 2018, the University of Maryland Applied Research Laboratory for Intelligence and Security (ARLIS) has served the Department of Defense (DoD) and U.S. Government as a strategic asset for research and development in the intelligence and security domains.

As a DoD-designated University Affiliated Research Center (UARC), ARLIS develops and maintains deep expertise in human and social systems, advanced computing and emerging technology, and integrated human-machine systems, along with operational expertise in missions across the intelligence and security enterprise. This blend of multi-disciplinary talent enables ARLIS to form uniquely qualified teams to solve problems at the intersection of technology, policy, and people.

ARLIS is a trusted resource for the DoD and intelligence community. By synthesizing project insights into operational strategies, we strengthen decision-makers' abilities to respond effectively to emerging threats. Our commitment to excellence and innovation helps ensures the nation remains agile in a rapidly evolving strategic landscape.

As the government confronts the critical intelligence and security challenges ahead, ARLIS is dedicated to enabling national security information advantage and decision superiority by developing scientific foundations and engineering sociotechnical capabilities in the human domain. Our mission-aligned initiatives solidify our role as a key trusted partner for applied research informing strategic competition and delivering solutions that secure our nation's future.

WHO WE ARE

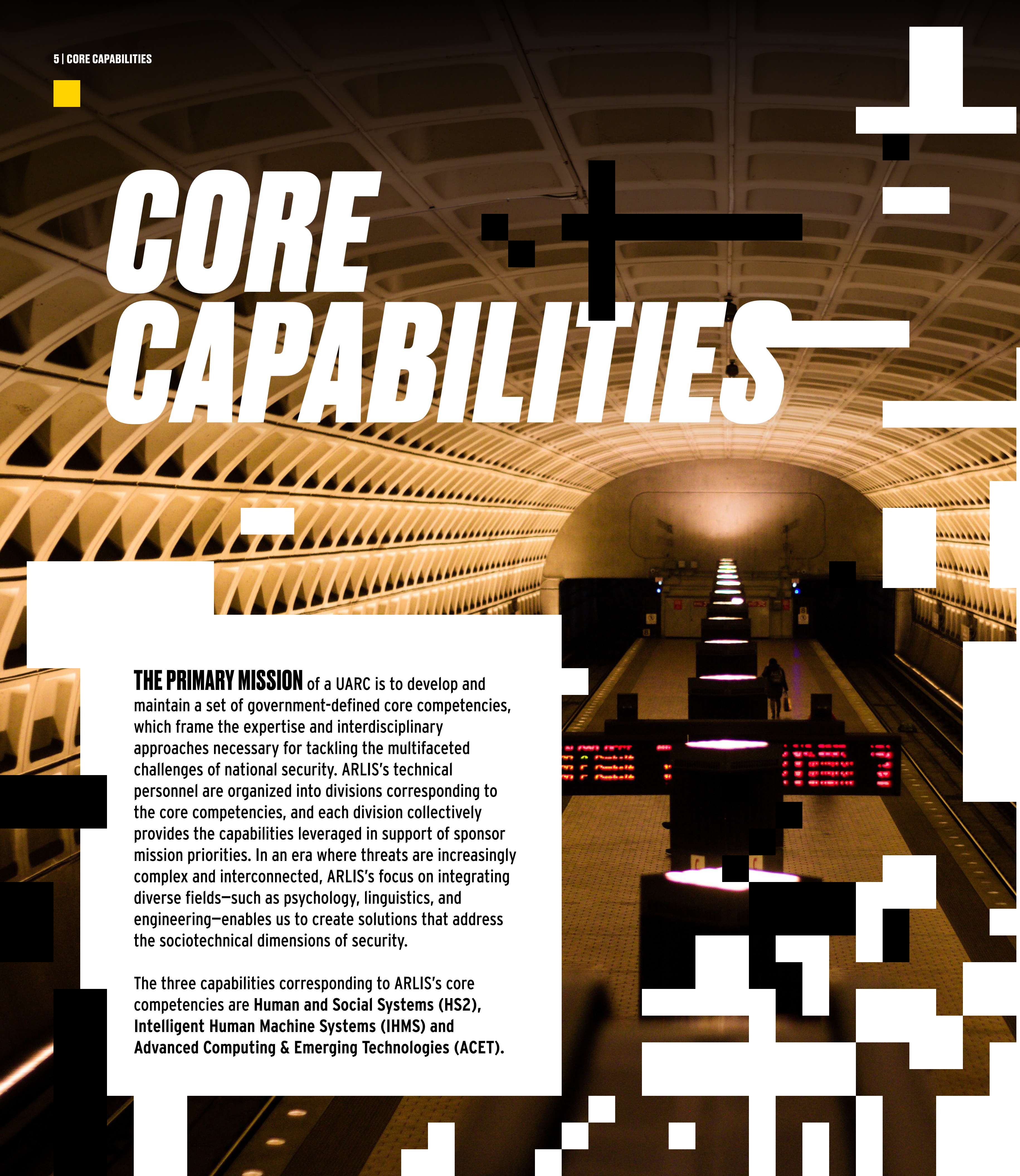


With more than 200 full- and part-time employees (nearly half with masters degrees and another 25% with doctorates), the ARLIS team continues to grow in diverse areas of expertise. Research disciplines span fields from engineering and systems design to artificial intelligence, machine learning, data science, security, political science, psychology, and human factors. This range of backgrounds helps our teams understand the complex multidisciplinary challenges faced by the defense intelligence and security enterprise.

A RECORD-BREAKING CONTRACT RENEWAL

In May, the U.S. government awarded ARLIS a record-breaking Indefinite Delivery/Indefinite Quantity (IDIQ) contract worth up to $500 million – the largest contract ever awarded to the University of Maryland. This contract marked the first renewal of ARLIS's UARC status since its inception in 2018, reinforcing our vital role in supporting national security missions.

The new IDIQ contract features a ceiling more than double that of the previous contract and over five times the original IDIQ ceiling. The increase reflects the government's confidence in ARLIS's ability to meet the growing demands of intelligence and security research in the coming years.



CORE CAPABILITIES

THE PRIMARY MISSION of a UARC is to develop and maintain a set of government-defined core competencies, which frame the expertise and interdisciplinary approaches necessary for tackling the multifaceted challenges of national security. ARLIS's technical personnel are organized into divisions corresponding to the core competencies, and each division collectively provides the capabilities leveraged in support of sponsor mission priorities. In an era where threats are increasingly complex and interconnected, ARLIS's focus on integrating diverse fields—such as psychology, linguistics, and engineering—enables us to create solutions that address the sociotechnical dimensions of security.

The three capabilities corresponding to ARLIS's core competencies are **Human and Social Systems (HS2), Intelligent Human Machine Systems (IHMS) and Advanced Computing & Emerging Technologies (ACET).**

DEVELOPING SOLUTIONS INFORMED BY SOCIOCULTURAL CONTEXT

The Human & Social Systems (HS2) Division brings together diverse fields—from psychology to computational social science, linguistics, and cultural expertise—to understand the complexities of human motivations and behavior. This expertise informs decision-making, enhances operational effectiveness, and supports national security.

CAPABILITIES

MODELING COMPLEX HUMAN BEHAVIOR	Employing advanced modeling techniques to simulate human decision-making processes and knowledge acquisition (individually and in groups), allowing national security strategies to anticipate and counter threats effectively.
EVALUATING HUMAN PERFORMANCE AND WORKFLOW	Developing human-focused performance metrics, for example, credibility, cognition, and understanding, to improve test and evaluation of advanced technology and help develop training programs that improve mission outcomes and operational readiness.
NATURAL LANGUAGE PROCESSING & TEXT ANALYSIS	Dissecting communication patterns by utilizing natural language processing and linguistic analysis to provide insights into cultural and contextual factors critical for intelligence operations. Also, identifying key signals via multilingual text analysis.
RELIABLE OPEN-SOURCE INTELLIGENCE	Pioneering test and evaluation concepts and aligning evaluations with DoD and Intelligence Community standards, bolstering the reliability of intelligence applications.
BEHAVIORAL INSIGHTS ACROSS ENVIRONMENTS	Studying human reactions in diverse environments, including cyber contexts, informing training and strategies to mitigate risks effectively.

With the capabilities offered through the HS2 Division, ARLIS applied research outcomes can better account for human behavior and social dynamics in critical intelligence and security missions.

ADVANCING INTELLIGENT HUMAN-MACHINE SYSTEMS

The Intelligent Human Machine Systems (IHMS) Division combines expertise from engineering, social, biological, computer, and physical sciences along with government and policy knowledge. The interdisciplinary approach embodied by IHMS centers research and development around people's needs, capabilities, and experience, supporting technology development and science in rapidly evolving environments.

CAPABILITIES

AI, ML, AND DATA SCIENCE TO INFORM DECISION MAKING	Harnessing AI for language processing, enhancing communication and intelligence capabilities to enable more efficient data analysis and interpretation, vital for timely decision-making. Applying information and data science to address critical government applications, facilitating data-driven decision-making.
EFFECTIVE HUMAN-MACHINE TEAM DESIGN	Contributing to the design and development of artificial intelligence, focusing on creating effective human-machine teams. Modeling and simulating human-machine systems and teams for predicting interactions and improving system designs to enhance human performance.
AUGMENTING HUMAN PERFORMANCE	Leading research in human performance and readiness, optimizing training and operational effectiveness, ensuring that personnel are prepared for the challenges they face. Evaluating human performance, behavior, and learning, identifying areas for augmentation to optimize training programs and improve overall effectiveness.
ANALYZING IMPLICATIONS OF NASCENT TECHNOLOGIES	Developing standards and metrics to evaluate the ethical, legal, and social implications (ELSI) of AI policy, ensuring that AI technologies are deployed responsibly and align with national values and security objectives.
MEASURING TECHNOLOGY CONTRIBUTIONS TO PERFORMANCE	Verifying and validating artificial intelligence, machine learning, and other innovative technologies applied to intelligence and security missions, including test and evaluation at multiple levels (e.g., assessing AI behavior in isolation and as it contributes to an autonomous system).

Through these diverse capabilities, IHMS plays a pivotal role in enhancing national security, ensuring that scientific advancements are effectively aligned with societal and operational needs.

FOSTERING INNOVATIONS FOR ASYMMETRIC ADVANTAGE

The Advanced Computing & Emerging Technologies (ACET) Division is dedicated to fostering innovations that provide asymmetric advantages in intelligence and security missions. By integrating expertise from various fields, ACET develops methods and tools to support national defense initiatives and enhance operational effectiveness. This approach ensures that technological advancements are aligned with strategic objectives and real-world applications.

CAPABILITIES

DATA CURATION AND VISUALIZATION FOR INTELLIGENCE OPERATIONS	Developing advanced tools to curate, analyze, and visualize government and publicly available data, enhancing support for intelligence and security missions.
AI TO ENHANCE ANALYST CAPABILITIES	Researching and implementing AI, machine learning, and natural language processing to improve the efficiency and accuracy of declassification analysts, ensuring more effective mission outcomes.
EVALUATING ADVANCED ELECTRONICS IN MISSION CONTEXT	Conducting rigorous testing and evaluation of advanced electronics inspired by quantum technologies, paving the way for future innovations in defense systems.
ROBUST AND SECURE QUANTUM	Evaluating system cybersecurity and researching secure algorithms on a two-node quantum computer, ensuring robust defenses against emerging cyber threats.
AUTOMATIC EVALUATION OF SECURE SILICON	Implementing automated processes to evaluate secure silicon, ensuring that hardware meets stringent security standards for national defense applications.

By leveraging these diverse ACET capabilities, ARLIS is at the forefront of technological advancements that enhance national security, ensuring that our strategies are effective and adaptive in an ever-evolving threat landscape.

MISSION IMPERATIVES

Research capabilities provide value in the context of solving problems. ARLIS government customers have areas of responsibility facing some of the most critical challenges across the defense intelligence and security enterprise. ARLIS project portfolios are largely organized by these mission requirements.

SECURING OUR INDUSTRIAL BASE & TECHNOLOGICAL ADVANTAGE

ARLIS recognizes that securing the acquisition process and protecting industrial assets are critical to national defense. The Acquisition & Industrial Security(A&IS) mission area focuses on developing strategies and frameworks to ensure the veracity of supply chains and the security of sensitive information throughout the procurement process. By implementing robust industrial security measures, ARLIS supports the defense sector in mitigating risks associated with espionage, fraud, and other threats. This approach strengthens the overall security posture of defense organizations.

MITIGATING INSIDER RISK

Insider threats pose significant challenges to organizational security. The Modeling & Mitigating Insider Risk(MINR) mission area emphasizes the importance of modeling and analyzing human behavior to identify potential insider risks before they manifest. ARLIS conducts comprehensive assessments and develops predictive models that inform strategies for risk mitigation. By understanding the factors that contribute to insider threats, ARLIS equips organizations with the knowledge and tools needed to foster a secure environment, enhancing both individual and organizational resilience.

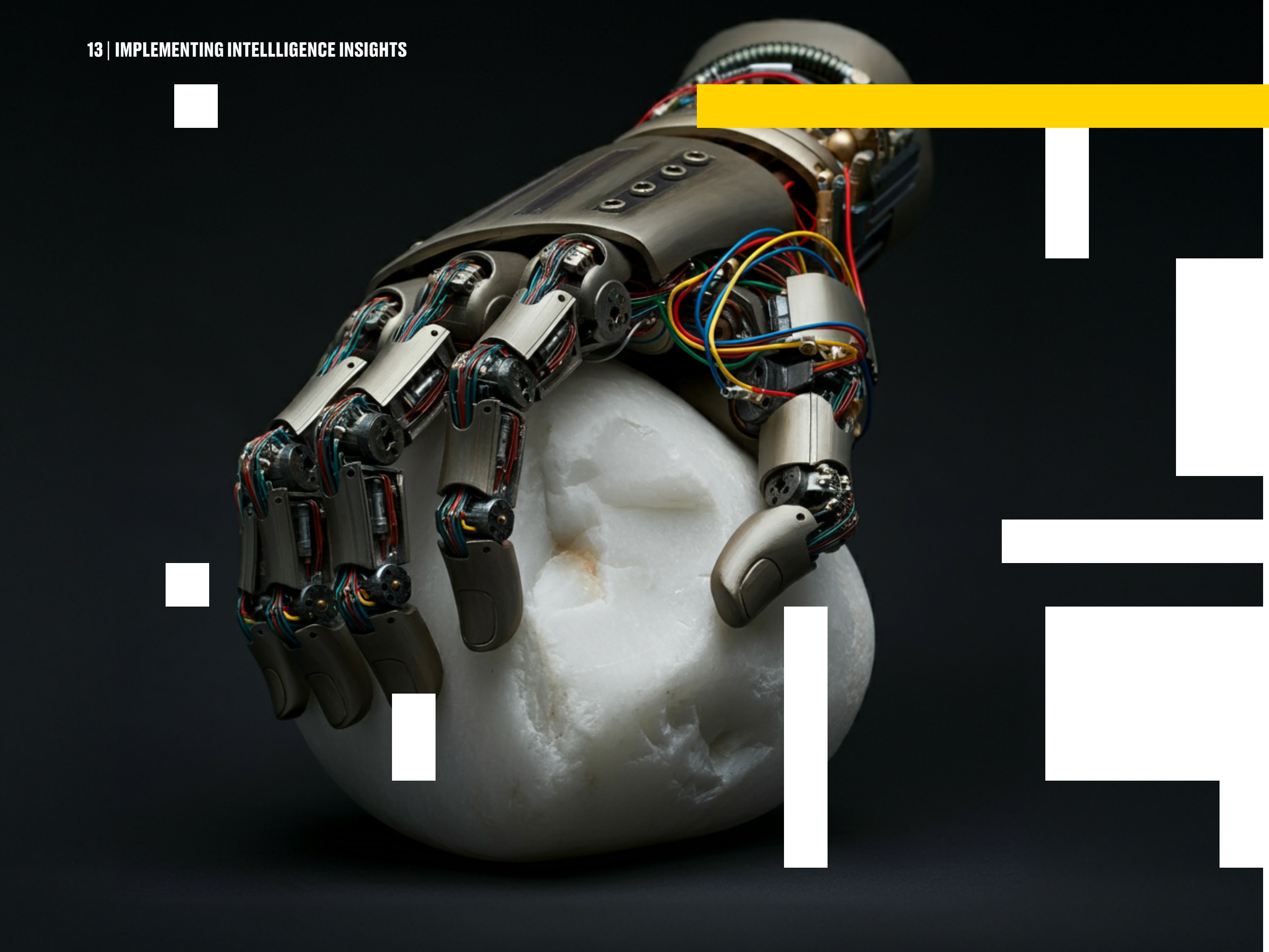
MISSION IMPERATIVES

OPERATIONS IN THE INFORMATION ENVIRONMENT

In today's modern age, maintaining accuracy and reliability of information is important for effective decision-making. The Cognitive Security mission area is dedicated to strengthening our ability to navigate complex information environments, countering attempts to disrupt trust or influence decision-making processes. ARLIS focuses on research to develop innovative tools and strategies that empower national security personnel to identify and address emerging threats in the information space. By addressing the evolving challenges posed by modern information operations, ARLIS helps ensure that decision makers are able to operate with confidence and precision in their environments.

COMMAND, CONTROL, ANALYSIS, & PERFORMANCE

The Command & Control, Intelligence, Surveillance, & Reconnaissance (C2ISR) mission area focuses on developing advanced AI systems that enhance decision-making and operational capabilities across various domains. By emphasizing the augmentation of human skills through autonomous systems, ARLIS aims to create continuous interactions between humans and machines, improving efficiency and effectiveness in complex environments. Rigorous research and development efforts are directed toward ensuring these technologies not only support military operations but also adhere to ethical standards and enhance mission outcomes.



IMPLEMENTING INTELLIGENCE INSIGHTS

ACQUISITION & INDUSTRIAL SECURITY

The Test-Bed Revolution

A team of dedicated researchers in the A&IS mission area has been developing testbed and augmentation-related prototypes designed to address the critical security concerns of government sponsors.

This exploration is not just about innovation; it's about safeguarding the very foundations of national security. With every prototype built, the team aims to enhance supply chain resilience and trustworthiness.

Critical Technology Protection Decision Framework

The Critical Technology Protection Decision Framework (CTP-DF) effort is enabling a decision-making capability that empowers policymakers to understand and make informed decisions about how to protect critical technologies to strengthen the U.S. innovation ecosystem and maintain strategic advantage.

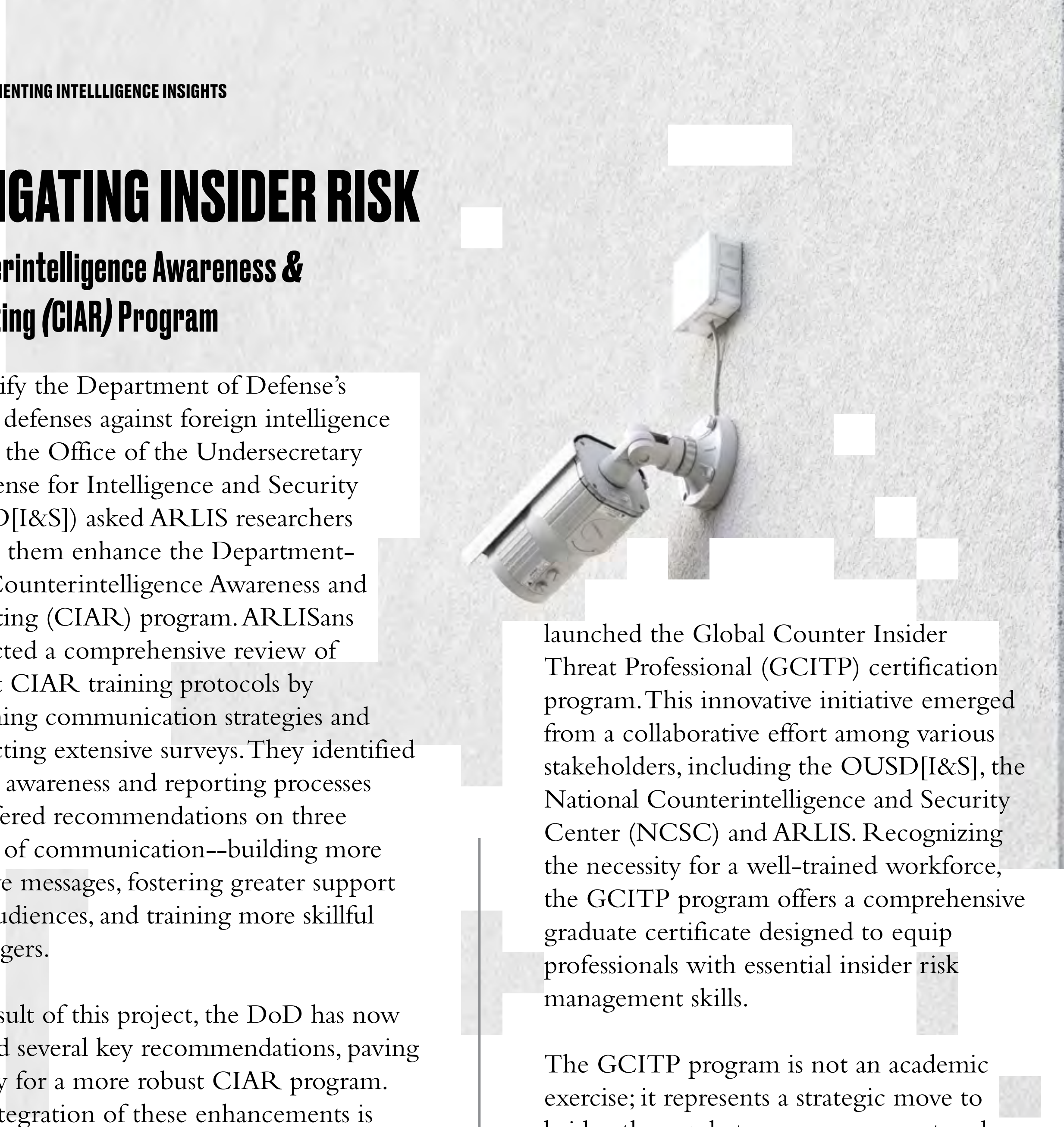
Decisions about technology protection are often influenced by subjective perspectives. This lack of objective analysis can lead to severe, unintended consequences that can stifle innovation and impair effective technology protection. The CTP-DF effort seeks to address these potential consequences by establishing an "Innovation Policy Lab" where potential policy impacts can be studied in a controlled setting. By using data and rigorous analysis, this lab provides insights that help policymakers understand the long-term effects of their decisions—ensuring that policies minimize risks and maximize desired effects to the U.S. technical innovation ecosystem.

Commercial Secure Facilities

The Commercial Secure Facilities project is developing a flexible testbed to understand how new technologies and approaches can be integrated to support shared collateral workspaces and Sensitive Compartmented Information Facilities (SCIFs). The goal is to enable commercially owned and operated secure facilities that government agencies and small enterprises can easily reserve and use.

Setting up new secure facilities can take multiple years and may often involve extensive modifications to existing buildings, becoming a major barrier to small businesses seeking to bring innovative security solutions to the market. This project enables a common operating model that allows commercial entities to offer secure spaces on a rental basis. While this model introduces new complexities—such as shared access by multiple users and distributed responsibilities—it also presents an opportunity to explore technologies for active monitoring and security. By using these testbeds, government agencies can experiment with different technologies and capabilities in a secure environment without the need to repeatedly modify collateral workspaces and SCIFs. This streamlines the process for testing new tools and supports mission-critical activities, providing resources for government leaders to enhance their operational effectiveness.

MITIGATING INSIDER RISK



Counterintelligence Awareness & Reporting (CIAR) Program

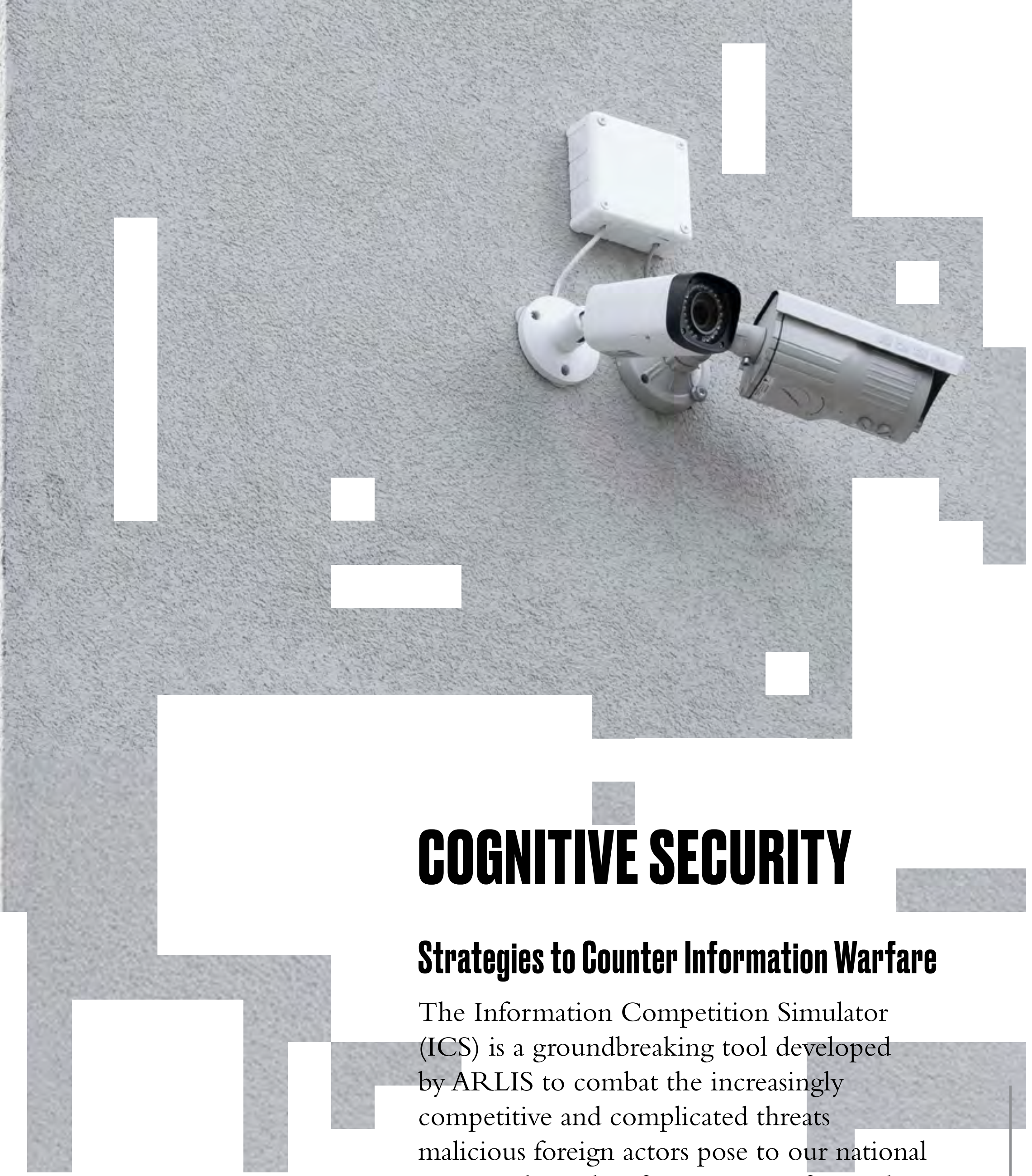
To fortify the Department of Defense's (DoD) defenses against foreign intelligence threats, the Office of the Undersecretary of Defense for Intelligence and Security (OUSD[I&S]) asked ARLIS researchers to help them enhance the Department-wide Counterintelligence Awareness and Reporting (CIAR) program. ARLISans conducted a comprehensive review of current CIAR training protocols by examining communication strategies and conducting extensive surveys. They identified gaps in awareness and reporting processes and offered recommendations on three aspects of communication--building more effective messages, fostering greater support from audiences, and training more skillful messengers.

As a result of this project, the DoD has now adopted several key recommendations, paving the way for a more robust CIAR program. The integration of these enhancements is expected to not only increase awareness but also foster a culture of proactive reporting among personnel, thus significantly bolstering the DoD's ability to mitigate insider threats. With the groundwork laid for a follow-on initiative aimed at further strengthening these practices, the 2024 conclusion of this project marks a pivotal step in safeguarding sensitive information and ensuring the integrity of the nation's workforce.

Global Counter Insider Threat Professional (GCITP) Certification Program

In response to a rising tide of insider threats and the critical need for standardized training, the MINR mission area has successfully launched the Global Counter Insider Threat Professional (GCITP) certification program. This innovative initiative emerged from a collaborative effort among various stakeholders, including the OUSD[I&S], the National Counterintelligence and Security Center (NCSC) and ARLIS. Recognizing the necessity for a well-trained workforce, the GCITP program offers a comprehensive graduate certificate designed to equip professionals with essential insider risk management skills.

The GCITP program is not an academic exercise; it represents a strategic move to bridge the gap between government and private industry in addressing insider threats. By developing a certification exam validated through rigorous Job Task Analysis, the program ensures that both sectors can adhere to common standards, enhancing credibility and professional identity within the insider threat community. With the program's formal launch in 2024, ARLIS is poised to expand its reach, creating impactful training opportunities that empower individuals to combat insider risks effectively. This initiative signifies a commitment to not only educate but also actively engage in reshaping the landscape of insider threat management, underscoring the importance of vigilance and preparedness in an ever-evolving security environment.



COGNITIVE SECURITY

Strategies to Counter Information Warfare

The Information Competition Simulator (ICS) is a groundbreaking tool developed by ARLIS to combat the increasingly competitive and complicated threats malicious foreign actors pose to our national security through information warfare and influence operations. As this threat landscape evolves, all elements of the national security apparatus recognize the pressing need for effective solutions.

This year, we made significant strides in expanding the ICS's capabilities and relevance. The simulator blends technology with social science, creating a training environment that replicates how information spreads and influences human behavior. It builds digital representations of specific populations, designed to mimic real-world behaviors, information consumption habits, and social interactions. This allows users to engage with simulated communities, bringing their own perspectives into the mix, which helps to illuminate how biases can impact decision-making in the realm of information warfare. ICS replaces dice rolls and pre-scripted outcomes in training scenarios with a dynamic and responsive population whose interactions with the training audience includes all of the nuance and human character of real populations. By refining the audience to mimic its real-life counterparts, it gives influence professionals and those who operate in the modern information environment hundreds of chances to make a good first impression before they are placed in a situation where high stakes national security implications are the norm. ICS is a teaching tool that actively engages information professionals in a realistic, robust environment and provides the challenges and detailed feedback that leads to rapid skill improvement.

In recent work with combatant commands and defense agencies, ARLIS provided course of action analysis and tailored simulations to meet their bespoke needs. Our involvement in the 2024 special operations forces capabilities exercise showcased the ICS's practical applications and effectiveness in real-world scenarios.

As we look to the future, the ICS is set to grow even further. We are working to integrate this innovative system into existing and emerging live virtual and constructive systems—a critical component for the next phase of development. This will enhance the simulator's robustness and solidify its role in training and operational strategies. Software and hardware integration will increase the usefulness of ICS, but we retain our strong human behavioral research into the complex mix of trust, emotion, bias, and media presentation that underpins the ICS and makes it unique. By continuing to refine and expand the ICS, we are ensuring that it becomes an integral part of the ongoing efforts to address the complex challenges posed by information warfare.

COGNITIVE SECURITY

Understanding Asymmetric Warfare

In the complex landscape of national security, traditional defense strategies often focus on tangible assets like tanks, airplanes, and missiles. However, the Asymmetric Threats Analysis Center (ATAC) was established to address the critical need for understanding the human element of security, particularly in asymmetric warfare. Recognizing that effective responses to modern threats require insight into human behavior, ARLIS has made it a priority to explore this often-overlooked dimension.

ARLIS remains the home of ATAC, which serves as the umbrella for a variety of projects focusing on social science, human-machine teaming, and their relevance to irregular warfare. These efforts also provide vital support to operators on the ground.

During this year's efforts, ATAC has placed a strong emphasis on examining the impact of AI on wargaming—a critical tool for analysis, planning, and training within the national security community. The rapid advancement of AI has complex implications for wargaming, prompting ATAC to explore both the potential benefits and the significant risks AI brings to this mission space.

The current wargaming project addresses two key areas:

1. Investigating innovative AI-driven technologies to enhance decision support, improve the validity of wargames, and increase their overall utility.
2. Conducting ethnographic research to better understand the wargaming landscape within the national security community, identifying opportunities to strengthen our capabilities against potential threats.

Through these efforts, ATAC is advancing national security by enhancing the understanding of asymmetric threats and preparing the U.S. for the complex challenges of the future.

COMMAND & CONTROL, INTELLIGENCE, SURVEILLANCE, & RECONNAISSANCE *(C2ISR)*

Test, Evaluate and Deploy AI for Intelligence Community Mission Success

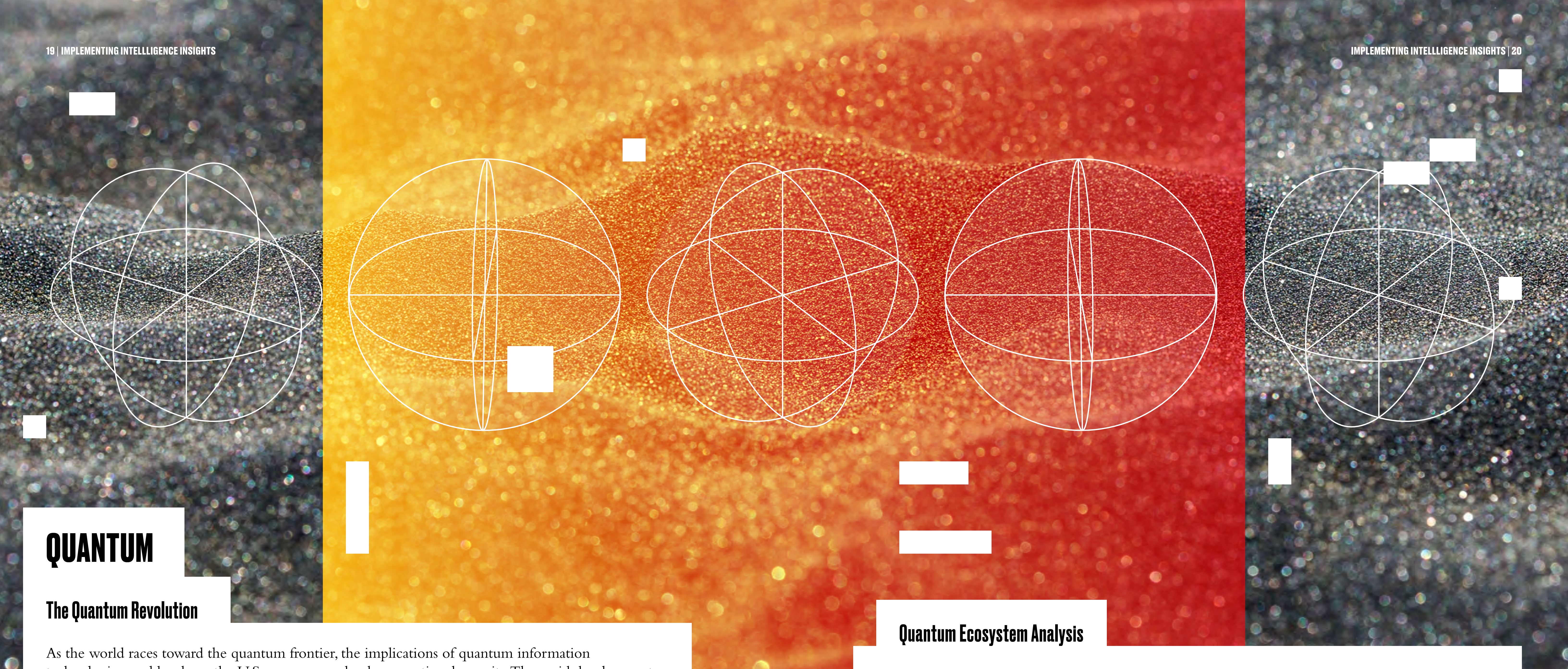
ARLIS is enhancing how the DoD and Intelligence Community (IC) evaluate and integrate AI-enabled systems through their work for the Chief Digital and AI Office (CDAO) and other sponsors. By focusing on robust test and evaluation (T&E) processes, ARLIS is reshaping the landscape of command and control, ensuring that emerging technologies are effectively deployed and assessed for their operational impacts. Recognizing the critical importance of understanding AI capabilities, our team is dedicated to moving beyond traditional assessments. By mapping workflows and identifying meaningful metrics, we foster a deeper understanding of operational environments, setting realistic expectations for AI applications.

Enhancing Human Machine Teaming and Adoption Through Operations Research and Analysis

ARLIS has created a comprehensive, modular data pipeline to support T&E and mission analysis for Combined Joint All-Domain Command and Control (CJADC2) systems, within the DoD and IC. This work leverages opportunities for system instrumentation that modern, digital planning and intelligence systems allow for. ARLIS' pipeline captures and processes native system logs to inform both system performance measures and operational impact assessments.

ARLIS' data processing pipeline supports a comprehensive framework for managing operational and technical risks throughout the lifecycle of advanced technologies, particularly AI-enabled systems. ARLIS has addressed gaps in the T&E community's methodology by creating new technologies that support operational risk assessment, including codifying workflows into searchable knowledge graphs. These graphs enable inference across human, technical, and procedural elements of operations, providing a basis for simulating operations based on test data. This approach reduces T&E overhead, delivering actionable results to developers sooner and helping program managers understand how new technologies integrate into broader CJADC2 concepts of operations, accelerating program startup.

ARLIS also develops technologies to instrument systems that lack native observability. By creating user and system telemetry tools in collaboration with open-source communities, we ensure that the DoD's vendor base has access to cost-effective, customizable tools for system and user observability, crucial for system certification. Our work addresses key operational issues, streamlines testing, and provides actionable feedback to developers.



QUANTUM

The Quantum Revolution

As the world races toward the quantum frontier, the implications of quantum information technologies could reshape the U.S. economy and enhance national security. The rapid development of quantum computing, sensing, and communication technologies is fueled by significant research and development efforts globally. ARLIS is providing essential resources and expertise to help government partners navigate this emerging field.

Quantum technologies use the unique properties of quantum mechanics to measure and process information in ways that regular devices cannot. These technologies could enable breakthroughs in cryptography, data processing, and sensing capabilities. As the landscape evolves, so does the necessity for an effort to ensure that the U.S. maintains its competitive edge.

ARLIS's Quantum Technology Program was established to bridge the gap between complex scientific advancements and practical national security applications. By collaborating with academic institutions, industry leaders, and government agencies, ARLIS is providing mission-informed support at the intersection of quantum science and security.

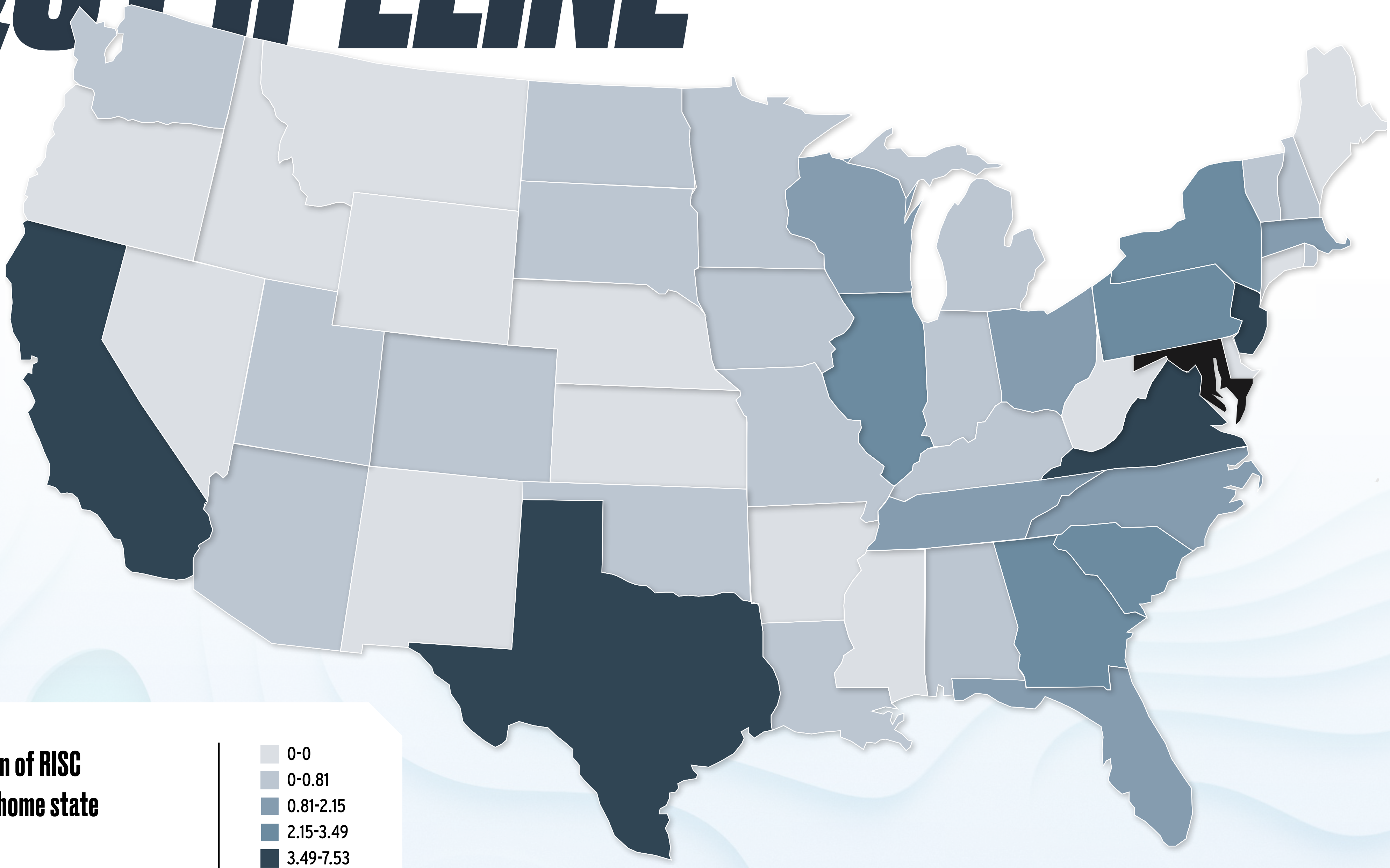
Quantum Ecosystem Analysis

Under the SEQCURE (Securing Experimental Quantum Computing Usage in Research Environments) effort, ARLIS also undertook various short- and long-term projects focused on analyzing trends within the domestic and international quantum information science ecosystems. With an in-house team of experts, ARLIS provided insights to its government sponsors, helping them sift through the noise surrounding quantum news and assess the potential impact of developments.

By analyzing patent data, publications, and funding announcements, ARLIS painted a clear picture of the current state of quantum innovation. The team produced reports that emphasized the federal government's role in driving Quantum Information Science research and analyzed technology development roadmaps published by quantum computer manufacturers.

As quantum information technologies advance, ARLIS is poised to play a role in ensuring that the United States remains at the forefront of this field. By fostering collaboration between academia, industry, and government, ARLIS is not only contributing to the national security landscape but also paving the way for innovations that could redefine the future of technology.

GROWING THE I&S PIPELINE



Distribution of RISC interns by home state

STUDENTS BY PERCENTAGE

THE RISC INITIATIVE

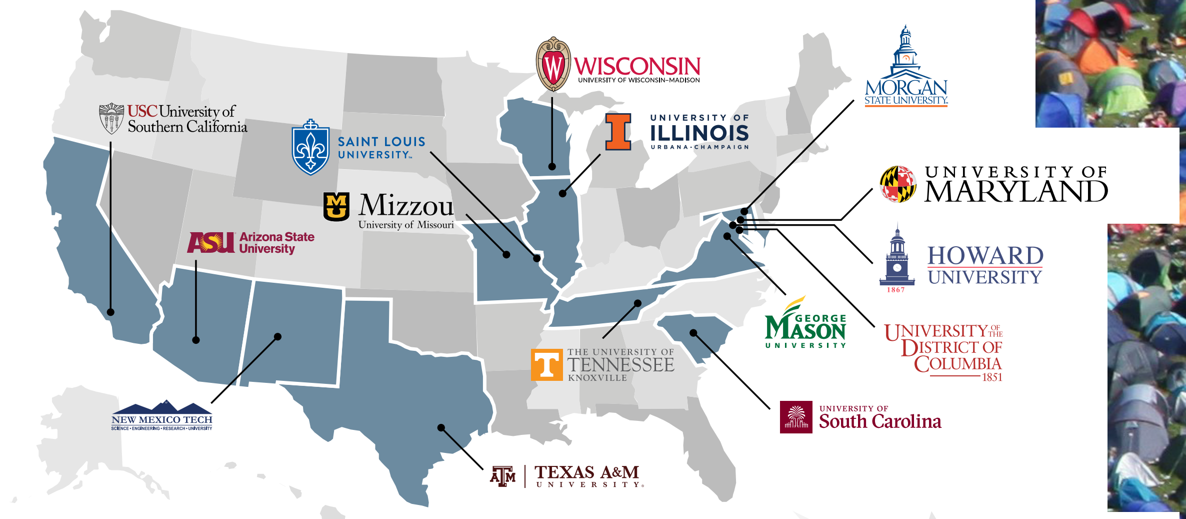
In 2020, ARLIS launched the Research for Intelligence & Security Challenges (RISC) initiative to help fill the deficit of government employees needed to address today's intelligence and security challenges, particularly those with training in Science, Technology, Engineering and Mathematics (STEM) fields and rigorous research-driven analysis.

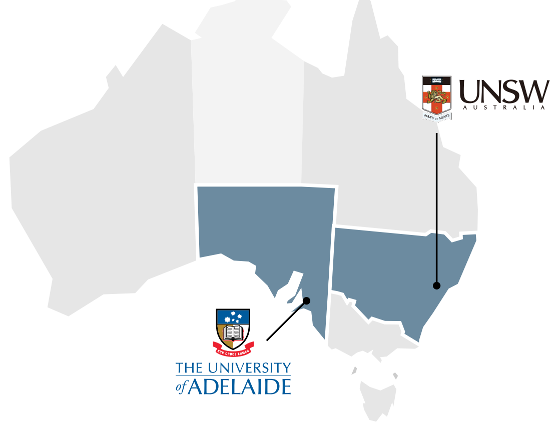
The ARLIS RISC internship program provides a pipeline of student talent at both graduate and undergraduate levels, providing students an opportunity to work on real-world problems within ARLIS focus areas.

Over an intensive 10-week mostly virtual program, competitively selected interns worked in teams of two-to-four students under guidance from faculty mentors and government topic champions. Government operators posed real-world problems supported with realistic data sets and other materials.

The program is structured to facilitate interactions within teams, between teams, and with government sponsor representatives. Interns attended weekly seminars and regular team development meetings in a shared virtual work environment, although select projects required on-site work. The summer program concludes with several days of in-person activities in College Park, Md., where attendees discussed project outcomes with peers and visiting experts from the defense and intelligence communities and gained greater context on how the work fits into government sponsors' mission space.

CULTIVATING COLLABORATION


USC University of Southern California
SAINT LOUIS UNIVERSITY
Mizzou University of Missouri
ASU Arizona State University
WISCONSIN UNIVERSITY OF WISCONSIN–MADISON
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN
MORGAN STATE UNIVERSITY
UNIVERSITY OF MARYLAND
HOWARD UNIVERSITY 1867
GEORGE MASON UNIVERSITY
UNIVERSITY OF THE DISTRICT OF COLUMBIA 1851
UNIVERSITY OF South Carolina
THE UNIVERSITY OF TENNESSEE KNOXVILLE
NEW MEXICO TECH
TEXAS A&M UNIVERSITY

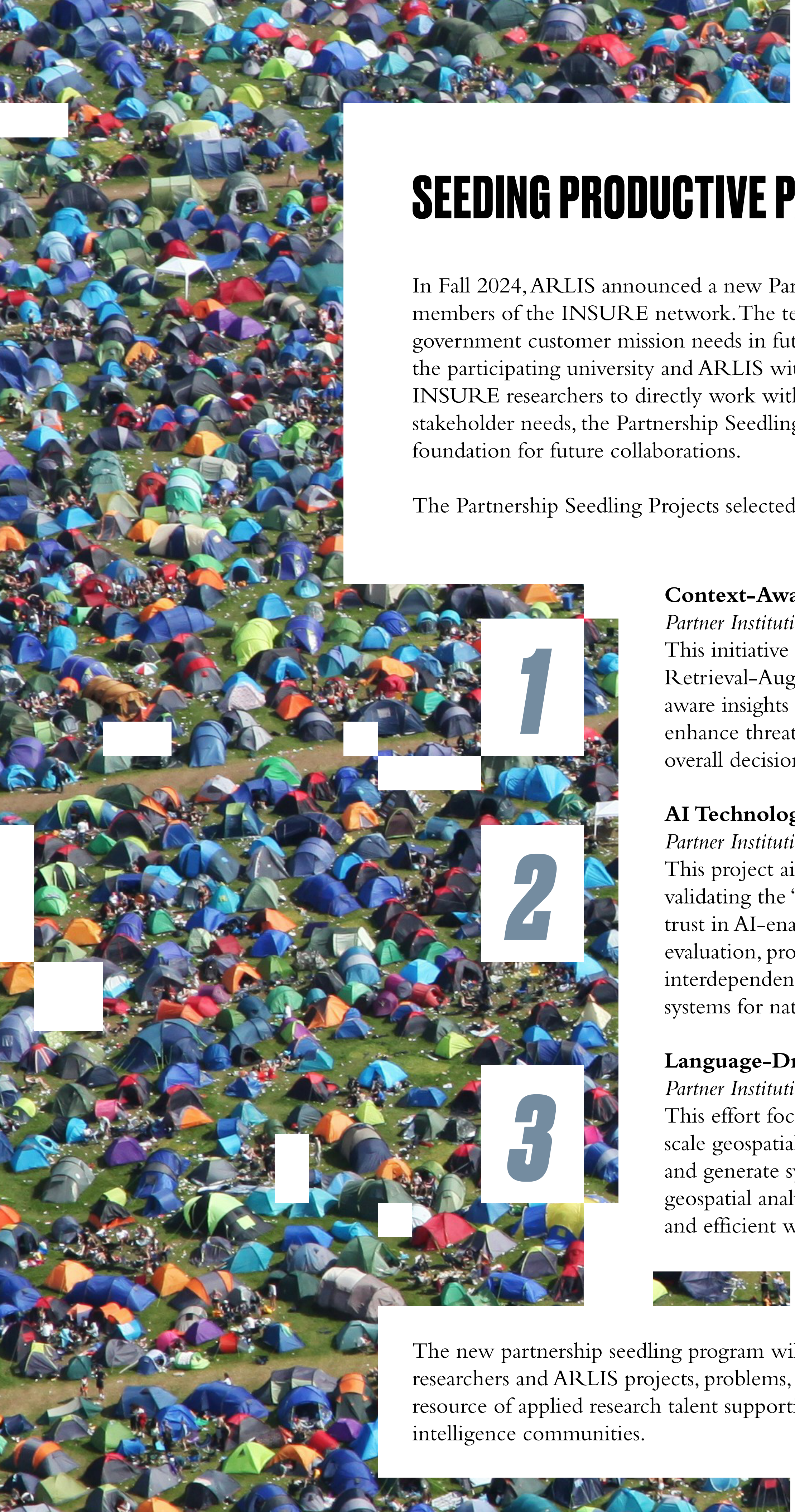


ARLIS launched the Intelligence and Security University Research Enterprise (INSURE) academic consortium in 2020 to expand the talent base and stakeholder reach required to advance its mission to serve as a national resource for the defense intelligence and security enterprise.

INSURE members include top R-1 research institutions around the country, working together with other strong research institutions too often left out of the defense innovation pipeline such as Historically Black Colleges and Universities and Minority-Serving Institutions. INSURE international affiliates in Australia share research findings in relevant topics to form a cooperative community of interest.

ARLIS and its partners coordinate applied and use-inspired research activities at member institutions, aligning projects with specific DoD and IC program managers and activities. This alliance improves the translation of projects into operational use and enhances the pipeline of students and faculty to work directly on technology problems for the national security community.

With 15 member institutions, INSURE is a resource enabling DoD and IC access to a wide range of vetted academic talent nationwide to solve critical problems.



SEEDING PRODUCTIVE PARTNERSHIPS

In Fall 2024, ARLIS announced a new Partnership Seedling program for current and candidate members of the INSURE network. The team solicited proposals for research to support U.S. government customer mission needs in future funded work while advancing collaboration between the participating university and ARLIS within priority growth areas. By facilitating opportunities for INSURE researchers to directly work with ARLIS principal investigators and learn about government stakeholder needs, the Partnership Seedlings will generate not only cutting edge research but a foundation for future collaborations.

The Partnership Seedling Projects selected for 2025 support are as follows.

1

Context-Aware Multimodal Information Retrieval Systems

Partner Institution: University of Wisconsin

This initiative combines Large Multimodal Models (LMMs) with Retrieval-Augmented Generation (RAG) to deliver real-time, context-aware insights for national security applications. The system aims to enhance threat detection, situational awareness, operational planning, and overall decision-making processes.

2

AI Technology Evaluation Study via Testbed (AI TEST)

Partner Institution: Arizona State University (ASU)

This project aims to improve understanding of human trust in AI by validating the "MASTOPIA" testbed, which measures context-dependent trust in AI-enabled systems. This testbed fills a gap in current test and evaluation, providing a cost-effective rubric that assesses the human-AI interdependencies that affect trust, a critical step in operationalizing AI systems for national defense.

3

Language-Driven Interaction with Geospatial Data

Partner Institution: Washington University in St. Louis

This effort focuses on enabling non-expert users to interact with large-scale geospatial datasets through natural language interfaces, to segment and generate synthetic satellite imagery. This research aims to help more geospatial analysts become better at their jobs, making them more capable and efficient when working on national defense and intelligence tasks.

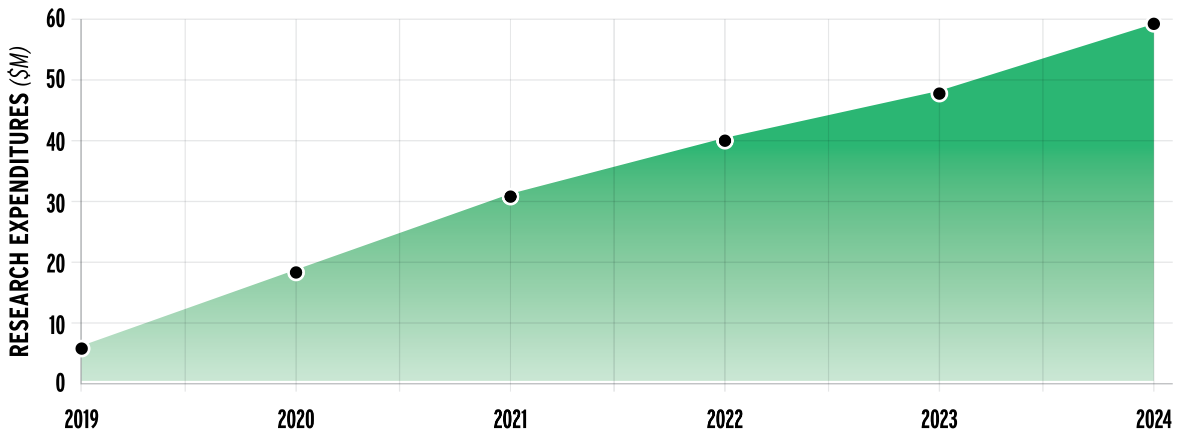
The new partnership seedling program will help strengthen connections between INSURE researchers and ARLIS projects, problems, and people, helping to grow INSURE into a national resource of applied research talent supporting ARLIS's UARC mission for the U.S. defense and intelligence communities.

FINANCIAL OVERVIEW

2024 saw the University of Maryland secure the largest research contract in its history. At the end of May, the DoD demonstrated its support for ARLIS with a new IDIQ contract, offering a five-year ceiling of $500 million.

The record setting award marks the culmination of nearly two years of collaboration between UMD and ARLIS's sponsoring agency, OUSD(I&S), aimed at achieving contract renewal. In just seven months, nearly 10% of the total ceiling has already been awarded, and ARLIS is on track to reach the $500M ceiling over the five-year ordering period. Additionally, ARLIS nearly doubled its awarded funding year-over-year for the first six months of the fiscal year (UM FY24 vs. UM FY25).

Moving into 2025, ARLIS is positioned to meet the DoD's research needs with more than 200 employees - a 10% increase compared to 2023. With trust and support from OUSD(I&S), ARLIS is building a trajectory to further expand its relationships across the DoD and IC.



WORKING WITH ARLIS

ARLIS exists to support the DoD and IC. As a UARC, ARLIS has the ability to enable sole source contracting in support of its core capabilities. To work with us, contact info@arlis.umd.edu

WWW.ARLIS.UMD.EDU
INFO@ARLIS.UMD.EDU