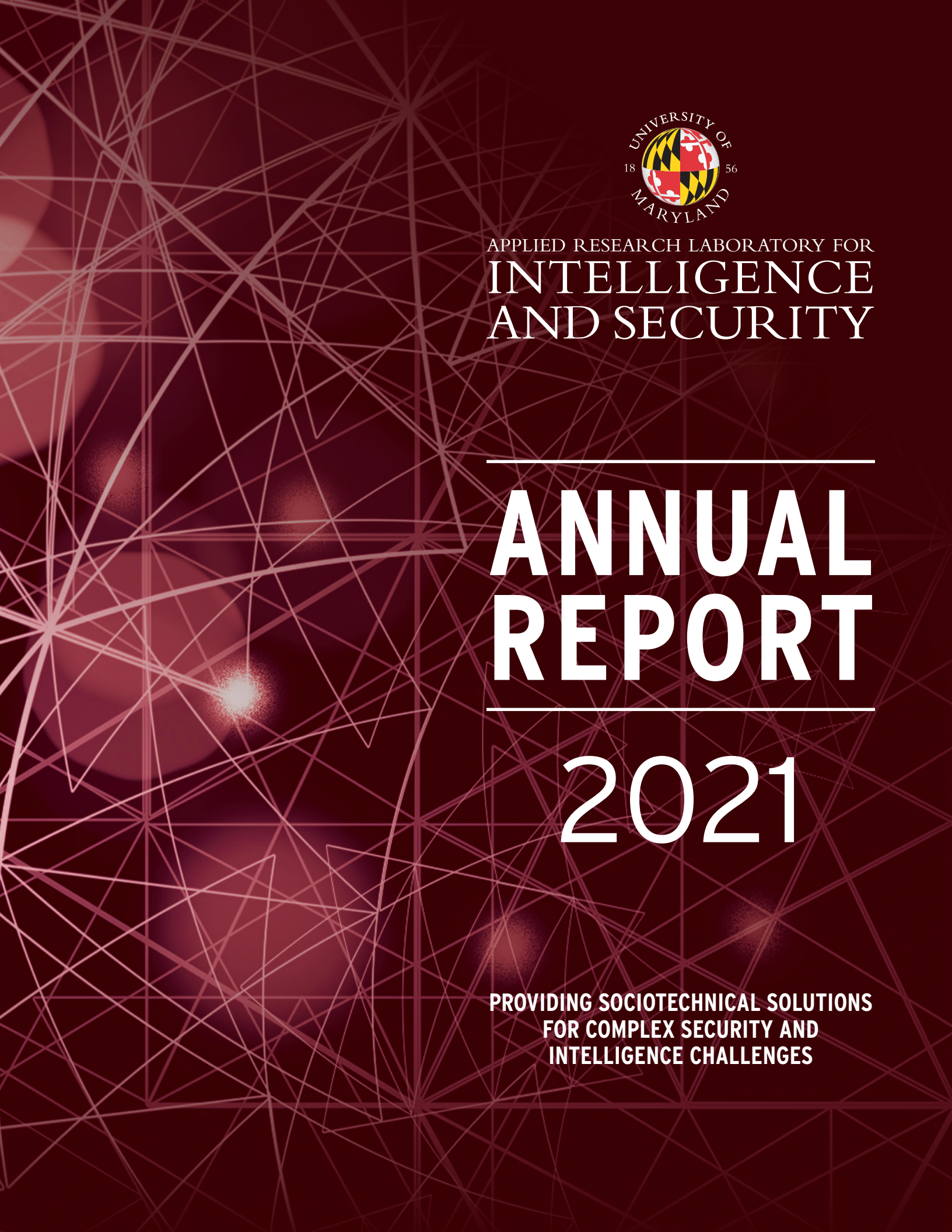


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

ANNUAL REPORT

2021

PROVIDING SOCIOTECHNICAL SOLUTIONS FOR COMPLEX SECURITY AND INTELLIGENCE CHALLENGES

From the Executive Director

ENABLING THE INTELLIGENCE AND SECURITY EDGE

As we close out 2021, we take stock of a year of growth beyond expectations and challenges vigorously met. Throughout the pandemic, ARLIS has remained steadfast in its goal to establish and maintain world-class science and technology expertise in areas of core competency to support national requirements for intelligence and security research.

ARLIS has deepened and broadened our team of scientists and engineers in critical areas of national security need, such as artificial intelligence, behavioral science, and information systems. Others have joined ARLIS with deep expertise in the mission areas for the intelligence and security communities, including counterintelligence, technology protection, and personnel security.

Support from our core sponsor, the Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S))—as well as strategic partners such as the Defense Intelligence Agency, National Geospatial-Intelligence Agency, and Defense Advanced Research Projects Agency—have populated a diverse portfolio of over 60 projects, from basic sciences in AI and microelectronics to operational support activities for combatant commands and agencies in the Defense Security Enterprise.

As we enter 2022, ARLIS is transitioning from "start-up" into a robust center of excellence for national security research. The evolving ARLIS represents a new type of University Affiliated Research Center (UARC) for the Department of Defense, with a core team of experts augmented by partners in the ARLIS-led Intelligence and Security University Research Enterprise (INSURE) consortium.

ARLIS addresses the personnel pipeline for the DoD and Intelligence Community (IC) by managing internship programs for the IC and by creating pathways into the national security workforce for undergraduate researchers as well as faculty and students at "non-R1" universities, such as Historically Black Colleges and Universities and liberal arts institutions.

Lastly, ARLIS establishes essential new resources for research, development, and operational transition in service to stakeholders across the government. These include computational support to provide controlled unclassified information (CUI) capabilities to the INSURE community, test and evaluation infrastructure for supporting the transition of AI technologies, and capabilities for processing public domain and commercial data sources—including sources across different languages—to understand global near peer competition and illuminate supply chains.

ARLIS is becoming an essential resource to the Department and stakeholders government-wide in addressing the most vexing sociotechnical national security problems facing the nation today. Thank you for this opportunity to share this 2021 overview of ARLIS with you.

William Regli, Ph.D.
Executive Director
Applied Research Laboratory for Intelligence and Security
University of Maryland

Contents

Making It Official: The ARLIS Ribbon Cutting

On December 2, 2021, following delays in gathering for an official ceremony due to COVID-19, University of Maryland officials were joined by Deputy Secretary of Defense Kathleen H. Hicks and Undersecretary of Defense for Intelligence and Security Ronald Moultrie to officially launch the Applied Research Laboratory for Intelligence and Security with a ribbon-cutting ceremony.

The esteemed speakers described a national need for an IC- and security-focused UARC, and UMD ARLIS's unique qualifications to serve in this role. Undersecretary Moultrie told the crowd, "The future of intelligence and security needs both advanced technology and advanced human understanding."

"We must better understand the human domain. We must ensure that we plan and account for both human strengths and human limitations."

"ARLIS will meet this challenge by taking a human-centered approach to intelligence and security matters," said Deputy Secretary Hicks. She continued, "By applying multidisciplinary methods to include social and technical sciences, ARLIS will take a strategic approach to innovation. It will focus on the protection of US technological, critical infrastructure, economic, and people and information priorities. It could not have come at a better time."

> "ARLIS will focus on the protection of US technological, critical infrastructure, economic, and people and information priorities. It could not have come at a better time."
>
> – DR. KATHLEEN HICKS, DEPUTY SECRETARY OF DEFENSE

> "The future of intelligence and security needs both advanced technology and advanced human understanding."
>
> – MR. RONALD MOULTRIE, UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY

Who We Are

Adversaries increasingly contest U.S. national security by imposing asymmetric risk through the information and cyber domains and throughout the supply chain. Solving these complex challenges for the intelligence community and the Department of Defense (DoD) requires a deep understanding of human and social systems, information science, and engineering, closely aligned with intelligence and security mission requirements.

The Applied Research Laboratory for Intelligence and Security (ARLIS), based at the University of Maryland College Park, was established in 2018 under the sponsorship of the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), intended as a long-term strategic asset for research and development in these areas. One of only fourteen designated Department of Defense University Affiliated Research Centers (UARCs) in the nation, ARLIS conducts classified and unclassified research that spans from basic to applied system development and works to serve the government as an independent, objective trusted agent.

By providing rigorously obtained scientific insights and sociotechnical solutions to hard security and intelligence challenges, ARLIS helps defense and intelligence mission owners respond effectively to these challenges and advance national objectives. To create pathways for continuing and greater impact, in 2022 ARLIS will publish a Five-Year Strategy (2022-2027), articulating the impact ARLIS intends to achieve by 2027 in each mission area and how we plan to get there.

ARLIS'S CORE VALUES

Our core values are meant to remind us—and signal to others—who we are, what we do, how we do what we do, and, most importantly, why we do what we do.

We believe our values are key to our success as an effective and healthy organization, a trusted partner, and a thriving community. We developed these values to help guide our behaviors and to have a "true North" to help maintain what makes us unique as we evolve into a critical applied research asset for the Nation.

HUMANS FIRST

ARLIS is building an enduring R&E capability to build solutions that help tackle complex national security problems—which are invariably human problems. We use technology to better understand and augment humans and sociotechnical systems for the benefit of the Nation. We create better solutions by keeping human diversity at the center of our research and our operations. So we also embrace teamwork as key to our success: we value—and celebrate— those who put the team first.

MISSION ALWAYS

We know that the "applied research" in our name is a beacon for making our work useful. It lends urgency to what we do: serving those who serve us by enabling them to better preserve and defend our democracy. We focus on mission impact by developing a deep familiarity with our sponsors and their challenges, ensuring that our work makes a lasting and positive contribution to the Nation. We also think long-term as we build our R&E capability, never forgetting that we are planting trees today whose shade may only be enjoyed by those who come after us.

TRUSTWORTHY TOGETHER

We understand that our mission puts us in a position that demands trust—from our sponsors, our partners, our country, and each other. We hold ourselves accountable to the highest research and ethical standards, and we keep the confidence of those whose mission depends on us. We treat ourselves and each other with respect, acknowledging everyone's inherent right to dignity, and we earn our trust every day through what we do.

> "The university is tremendously proud of this collaboration with the Department of Defense and grateful for the opportunities it awards our faculty and students to help address ever-evolving threats to national security and to shape the intelligence and security workforce of the future."
>
> – DARRYLL J. PINES, PRESIDENT OF THE UNIVERSITY OF MARYLAND

TRUSTED SERVICES

ARLIS aims to be a trusted partner for our government sponsors, ensuring that they have the bench—the capabilities, the expertise, and the skill sets—available to them to help address their needs and solve their problems.

A key tenet of being a DoD-designated UARC is operating in the public interest as a strategic partner with government sponsors rather than, for example, in the interest of corporate shareholders. ARLIS conducts business in a manner befitting its special relationship with DoD, combining technical excellence with independence and objectivity.

ARLIS's role as a UARC enables a strategic relationship with our sponsors that allows unique access to their operational contexts and information, resulting in deeper knowledge of sponsors' needs and greater opportunity for impact.

In 2021, ARLIS supported six significant Test and Evaluation or Independent Validation and Verification efforts for major funders of federal research. ARLIS technical staff also contribute as trusted subject matter experts in several ways: providing software and analysis support services, shaping future government programs, and taking on roles within the federal government through Intergovernmental Personnel Act (IPA)-enabled detail assignments.

STRATEGIC PARTNERSHIPS AND THE INSURE CONSORTIUM

Building teams to support government sponsors on their most critical sociotechnical challenges requires ARLIS to be agile and creative. Above all, as a resource to the nation, ARLIS must allow the problem at hand to define the team rather than letting the team available constrain the problem tackled.

Aggressive hiring (see "Our People") is only one component of our talent acquisition strategy. In management, Joy's Law is the principle that "no matter who you are, most of the smartest people work for someone else" (Bill Joy, founder of Sun Microsystems). With this in mind, ARLIS has stood up the Intelligence and Security University Research Enterprise (INSURE) academic consortium, a network of trusted university partners to expand and deepen ARLIS's bench of expertise available in service to its government customers.

ARLIS partnerships extend beyond INSURE. We have a growing number of collaborations with other UARCs and FFRDCs along with small companies and non-INSURE universities. On the international front ARLIS partners with institutions in the U.K. and Australia, and in fact in Fall 2021 the chief scientists from the Ministries of Defence for both countries came to UMD to meet with ARLIS and discuss mutual interests.

PART OF A WORLD-CLASS UNIVERSITY

ARLIS's strengths are reflective of the larger strengths across the University of Maryland campus. Inspired by its land-grant mission legacy, the University of Maryland honors its commitment to develop research, educational, and technological strengths to positively impact the quality of life, not just locally but worldwide. The benefits of UMD's land-grant tradition have given ARLIS a clear mission to not only create purpose-driven research to address some of our country's most difficult challenges but also to nurture a pipeline of future scientists and build academic partnerships with higher learning institutions nationwide.

UMD has 41,200 students, 4,200 faculty, and in 2019 (after UMD-College Park research merged with UMD-Baltimore) recorded $1.1 billion in federal expenditures. The University is recognized for its diversity, with underrepresented students composing one-third of the student population of undergraduate and graduate students.

UMD's state-of-the art research capabilities and facilities, coupled with its prime location—just seven miles from the

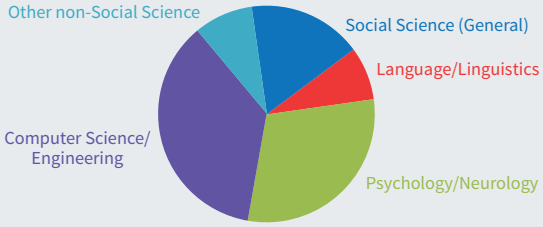
OUR PEOPLE

Critical to generating robust analysis and trusted tools in the human domain is the ability to create true multidisciplinary and interdisciplinary teams, grounded both in the technical state of the art and a direct understanding of the complex challenges faced by the defense security and intelligence enterprise.

The ARLIS research team draws from a wide range of expertise and disciplines, as listed below. Their background in these disciplines supports our work in areas such as artificial intelligence, behavioral science, information systems, and intelligence and security, among others. These technical experts work with former and current defense security and intelligence operators and policymakers to solve difficult national security problems, resulting in quality research that is relevant both to academia and our operational partners.

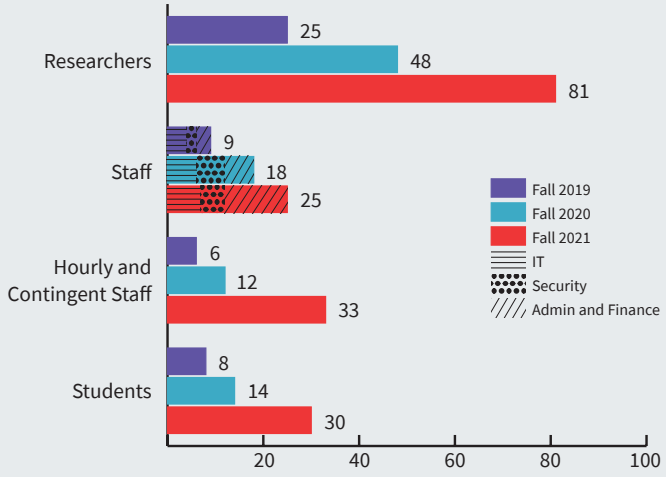
ARLIS's diverse group of researchers, scientists, engineers, and security experts continues to grow. **In 2021 we hired seven engineers, nine scientists, two postdoctoral associates, six professors of practice, and eighteen other faculty and staff.**

OVER 40 DIFFERENT DEGREES AND DISCIPLINES



Aerospace Engineering Arabic Language & Literature Biomedical Engineering Business Administration • Chemistry Civil Engineering Clinical Psychology • Cognitive Psychology Computer Science Cultural Anthropology Economics Measurement, Statistics & Evaluation Electrical Engineering Experimental Psychology French Government, Politics & Strategic Studies • History • Human Factors/Human Computer Interaction Industrial Engineering Information Systems Intercultural Studies • International Relations Japanese • Linguistics Mathematics Mechanical Engineering Neuroscience Nuclear Physics • Physics Political Science Psychology Public Administration • Public Policy • Rhetoric & Professional Communication Russian Social Anthropology Space Science & Applied Physics Spanish Visual Communications

ARLIS GROWTH



ARLIS TEAM PROFILES

ERICA BRISCOE

Title: Chief of Science and Technology Strategy

Joined: May 2021

Previous role: Chief Technology Officer, Georgia Tech Research Institute

Why did you join ARLIS? To work with others that equally appreciate the science of humans and cognition towards solving complex problems.

JOSHUA POORE

Title: Associate Research Scientist

Joined: February 2021

Previous role: Senior Principal Scientist and Technology Development Manager, BAE Systems, Inc. FAST Labs

Why did you join ARLIS? To work in collaboration with data scientists, user researchers, system engineers, and incredibly bright UMD students to transform Human-System Integration testing to an operations-grounded, replicable practice.

WILLIAM STEPHENS

Title: Director, Counterintelligence Research; Mission Area Coordinator, Insider Risk Research

Joined: January 2021

Previous role: Director, Counterintelligence, Defense Counterintelligence and Security Agency; AFOSI Colonel, 27 years USAF Service

Why did you join the ARLIS team? My 38 year career before coming to ARLIS was "wild fun" and ARLIS represents the best opportunity to continue contributing to the CI and Security world in an academic institution of considerable influence. I love this place and this opportunity.

MATTHEW VENHAUS

Title: Mission Area Coordinator for Cognitive Security and Operations in the Information Environment

Joined: April 2021

Previous role: Senior Principal Cyber Operations Engineer, The MITRE Corporation

Why did you join the ARLIS team? To advance the art and science of cognitive security and build bridges between meaningful research and operational employment for new capabilities and strategic approaches.

U.S. Capitol—and status as the largest university in the Washington Metropolitan Area, have facilitated extensive strategic research partnerships with U.S. federal agencies, positioning UMD as the Nation's research university. In the immediate neighborhood are numerous government agencies devoted to scientific research, including the Army Research Laboratory, the U.S. Army's primary facility for scientific research; NASA Goddard Space Flight Center; the National Institute of Standards and Technology; the Food and Drug Administration; National Oceanic and Atmospheric Administration; and the National Security Agency. These strategic research partnerships with the federal government offer unique opportunities for students and IC professionals to work alongside ARLIS researchers to create new academies and foster internship programs.

Campus Partnerships

ARLIS collaborations with and for campus researchers serve as force multipliers for both groups. Campus affiliates contribute directly to ARLIS-led research and programs, offer technical perspectives to program development, and bolster ARLIS's strategic scientific vision by providing guidance on and access to cutting-edge research developments worldwide. In 2021 there were 16 ARLIS campus affiliates in addition to four non-campus and non-consortium ARLIS affiliates.

In turn, researchers at ARLIS contribute to UMD success broadly through participating in campus-led initiatives (such as the $68M Army Research Laboratory collaborative agreement known as AI and Autonomy for Multi-Agent Systems (ArtIAMAS)), holding joint appointments with academic units, teaching classes, and mentoring and advising students

Facility and Research Infrastructure

ARLIS's 128,000 square-foot secure workspace facilitates ARLIS work at all levels of classification and provides our government partners with secure access to our mission area capabilities and breakthrough scientific research.

Conveniently located in the National Capital Region, the ARLIS facility has proven to be a uniquely advantageous venue for hosting conferences and wargaming exercises year-round. Its 180-person auditorium and and 80-person conference room, both with secure video teleconferencing (VTC), support multi-participant meetings at the classified level. The facility is ideal for wargaming exercises as well, with multi-room real-time and adaptive gameplay infrastructure. For three years running, ARLIS has supported a series of high-visibility cyber-resilience exercises for the government, both technically and as event host.

Research infrastructure of course encompasses more than physical space. ARLIS is building a diverse and scalable multi-domain, multi-tenant computational infrastructure to better integrate research projects and capabilities from both academia and government. Existing projects like the Cognitive Security Proving Ground and the "Digital Twin" model for supply chain security require particularly robust IT infrastructure and the ability to interface with the systems of DoD and IC sponsors. ARLIS infrastructure (especially our NIST SP 800-171-compliant environment for controlled unclassified information) serves as a critical enabler for INSURE consortium members and other partners. Many partners do not have the ability to handle CUI in-house, which greatly limits the type of unclassified trusted work they could contribute to without ARLIS partnership.

> "Imagine how much harder physics would be if electrons could think."
>
> – MURRAY GELLMANN

> "Imagine how much harder physics would be if electrons had feelings."
>
> – RICHARD FEYNMAN

Current Mission Areas

While ARLIS's core technical capabilities provided to the government as a UARC stay constant over time, our sponsored research and development programs focus on the prevailing whole-of-nation challenges of the day. These clusters of programs with a common mission focus, or mission areas, are driven by critical problems faced by the security and intelligence communities, while seeking to be anticipatory and strategic rather than reactive.

In 2021, the principal ARLIS mission areas were **Enabling Cognitive Security**; **Modeling & Mitigating Insider Risk**; **Acquisition & Industrial Security**; **Operationalizing AI, Autonomy, & Augmentation**; and **Analytics & Tools for Languages & Social Systems**.

BIG SECURITY CHALLENGES IN 2021

2021 held many challenges for the U.S. and international community alike, several closely aligned to ARLIS mission areas. We have worked to decompose the complex problems and forge a way ahead, developing scientific understanding and sociotechnical solutions in support of major societal challenges including but not limited to disinformation surrounding COVID-19, supply chain operations, and ensuring a trusted workforce.

COVID and Disinformation

COVID-19 affects the USG's global relationships and the international information environment. To support U.S. response to challenges surrounding the pandemic, ARLIS has been conducting academic research on the International Information Environment, emphasizing online disinformation surrounding COVID-19. Research focus areas include research on mis- and disinformation campaigns, the attitudes and perceptions of adversaries toward the U.S. response to COVID-19, the impact of COVID-19 on international relations, counter-messaging to support allied vaccination efforts, and research on norms related to pandemics, infectious diseases, and chemical and biological warfare.

In addition, ARLIS is conducting detailed research on current biotechnology programs and their relevance to future USG capability development. This research will involve identifying and collecting relevant scientific reviews related to emerging technology developments as a result of the pandemic. It connects ARLIS's expertise in the Information Environment with technology, biology, social science, and political science. Understanding current international impacts of COVID-19 will help the USG prepare for future information conflict as well as potential infectious disease outbreaks and pandemics.

International Supply Chains

In 2021 international supply chain operations were disrupted by complications and impacts of the COVID-19 pandemic, causing worldwide shortages and affecting consumer purchasing patterns. These shortages were caused by a myriad of interrelated factors, including years of efficiency-focused process modifications, worker leave and unemployment, and the shifting needs of consumer demand patterns. However, inconsistent approaches to monitoring, managing, and mitigating supply chain risk creates a difficulty in communication and collaboration among participants to implement a resolution for supply chain operation challenges.

Addressing challenges in supply chain operations and supporting the mitigation and resolution of industry shortages and supply chain disruptions were priority goals in the ARLIS Acquisition & Industrial Security mission area prior to COVID and have only increased in significance. One such effort is the development of a modeling and simulation capability to encourage a common understanding of supply chain structure, operations, and impact. This simulation project supports USG concerns surrounding supply chain operations by speeding up the process of creating simulated environments and integrating all-source data and illumination methods to provide decision advantage related to risk and operational security. The safe and secure acquisition of products, data, and technology are a priority at ARLIS.

Trusted Workforce

In 2021, the defense security enterprise expanded efforts to counter insider threats, cull domestic violent extremism, clear an influx of refugees for admittance to the U.S., and shift toward continuous vetting for a growing population of cleared personnel. Accordingly, the need to assess with confidence who can be trusted and where hidden threats may lie has become more pressing.

To address these challenges, ARLIS researchers are working to validate that current processes are measuring the things that matter in the end. We are conducting new research and development to inform evidence-based assumptions about risk, building robust frameworks for test and evaluation of technological solutions proposed by industry, and developing new courses for training and education.

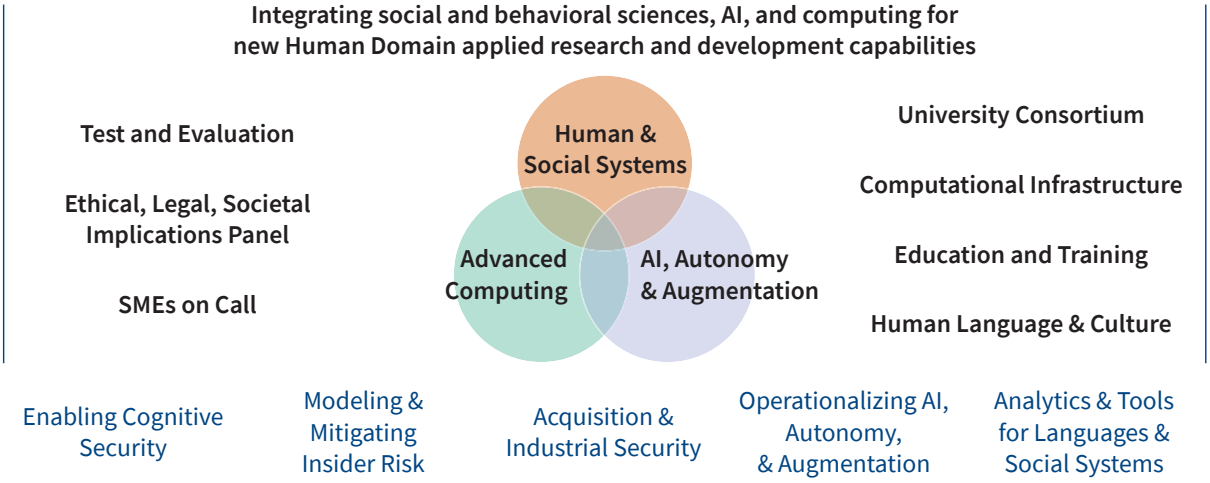
Beyond research, ARLIS personnel are working with security leads at other UARCs, Federally Funded R&D Centers (FFRDCs), and the INSURE consortium partners to understand existing research protection protocols at those institutions and design a pilot program to better balance real challenges faced at universities protecting information with the realities and requirements of an academic workplace.

THE UARC FOR THE HUMAN DOMAIN

ASSURING US AND ALLIED ADVANTAGE IN THE HUMAN DOMAIN

The Human Domain: where understanding and designing for human diversity—behaviors, beliefs, values, strengths, limitations, and vulnerabilities—confers competitive advantage in "Computing, Code, Cognition, and Communities"

Integrating social and behavioral sciences, AI, and computing for new Human Domain applied research and development capabilities



Cognitive Security and the Information Environment

Strategic control of the information environment, particularly online and offline influence at scales ranging from individuals to large societies, is a critical issue of our time. ARLIS attends to the challenges of Operations in the Information Environment (OIE) within the context of our Cognitive Security mission area, or COGSEC.

Our adversaries, competitors, partners, and allies are all engaged in OIE activities, which continue to grow in scope, scale, and importance. Due to advances in technology and information-sharing, all operations are made more complex by the unofficial information circulated about them, rendering every operation an operation in the information environment. To be successful, we must advance our understanding of how information operates within specific contexts.

The increased movement toward symbiotic human–machine interfaces create an even more urgent demand for research on information to inform operations in the broadest sense. The ARLIS COGSEC program leverages a multidisciplinary team and unique facilities to develop both targeted projects and overarching capabilities for a broad range of research, wargaming, and operational challenges, with goals including the following:

- Designing online systems and interactions to reduce vulnerability to misinformation and manipulation
- Detecting and mitigating targeted information manipulation attempts targeted at government insiders and
- Developing the integration of cyber and social media systems or simulations while also monitoring factors outside social media environments.

LINES OF EFFORT

The current constellation of ARLIS COGSEC activities spans applied research and engineering projects, test and evaluation efforts and frameworks, simulations and wargaming, and transition and training activities. Examples of each line of effort are detailed below: the Cognitive Security Proving Ground (T&E), the Languaculture Virtual Assistant for Strategic Communications (research), and the Phoenix Challenge Conference series (transition and training).

Cognitive Security Proving Ground

Despite the growing body of research tied to disinformation and mechanisms of influence, the community lacks a comprehensive technical environment for scientific study, test, evaluation, and wargaming of information and influence operations. In 2021 ARLIS completed the design and demonstrated the concepts and capabilities for a Cognitive Security Proving Ground (CSPG) for human behavior and influence.

The CSPG is a constellation of capabilities, locations, labs, ranges, and activities working in harmony. The desired endstate of the CSPG is a test and evaluation capability for the USG against a broad range of strategic and tactical questions for applied and operational research, wargaming, and mission support to ensure information advantage and the cognitive security of the Nation. Users both inside and outside of ARLIS will be able to select the appropriate resources, subject populations, data, capabilities, infrastructure, and modeling and simulation environments for their needs.

At the autumn demo event, researchers highlighted new test environments, such as a functioning social media simulator, and talked through the concept of operations (CONOPS) via a range of use cases, seeking the input and advice of the community of practice in an effort to better tune the CSPG toward operational relevance. The CSPG will enhance research and engineering in cognitive security and operations in the information environment, spanning scales from the individual to the whole of society. Once live, the framework will allow the fast-turnaround study of OIE questions within a secure environment, working with realistic system complexity, and producing actionable empirical results.

Languaculture Virtual Assistant

The Cognitive Security and OIE mission area works toward countering threats against the USG, such as influence campaigns. ARLIS is developing preventative measures, technology, and research addressing foreign malign influence to secure information advantage for the U.S. The Languaculture Virtual Assistant for Strategic Communications project focuses on enhancing U.S. strategic communications via a computer-based virtual assistant partnered with a human expert. Combining the advanced features of a virtual assistant with the robust knowledge and decision-making abilities of a human expert, we may acquire and use knowledge about language and culture, specifically regarding the large-scale communication involved in widespread social media use.

The technological tools used in this virtual assistant help extract stances that are indicative of people's beliefs about a topic, relevant to influence campaigns and countering and anticipating foreign malign influence. First, the adversary's influence campaigns must be detected—who is leading the campaign, what narratives are they pushing, and what are the topics of the campaigns? Then, the target audiences of the campaigns must be identified and analyzed. Finally, the effectiveness of the campaign with the given target audience must be analyzed as well. This sensemaking is key to taking action within social media and the information environment at large.

Phoenix Challenge 2.0

As progress is made in research and robust test and evaluation for cognitive security, ARLIS and the larger community need a venue to exchange ideas on best practices and new projects and to hold itself accountable for making progress on urgent issues relating to OIE. In 2021 ARLIS and the Information Professionals Association collaborated to revive the Phoenix Challenge Conference series.

Once organized annually by the IC but halted in 2013, the Phoenix Challenge is one of the only events to bring together military, intelligence, interagency, allied, academic, and industry participants across broad domains of expertise. The 2021 conference had over 300 attendees including senior defense leadership, developing themes in consultation with representatives from OSD, the Joint Staff, the Combatant Commands (especially USCENTCOM), Army, Navy, and Air Force, as well as the National Counterterrorism Center and the State Department's Global Engagement Center. Sessions ranged across all levels of classification and were held under Chatham House rules to encourage candid discussion.

ARLIS has confirmed future sponsor support to continue the Phoenix Challenge as a unique venue to propose new approaches and to hold itself accountable for making progress on urgent issues relating to securing the information environment.

> "The fight today is an information fight. What is our message, how are we communicating our message, are we aggressive enough with our message, and do we understand how to measure the impact?"
>
> – MAJOR GENERAL (RET.) LORI REYNOLDS, USMC

Modeling and Mitigating Insider Risk

Common to both defense security and intelligence community mission space are the goals of anticipating, avoiding, and mitigating damage resulting from insider threats. Being the UARC for these communities as well as the UARC with core competencies tied to sociotechnical systems, ARLIS is well-positioned to contribute high-impact research and development related to Insider Threats.

SHIFTING PARADIGMS

Identifying insider threat—and building a robust and validated process for vetting a trusted workforce broadly—is critical for national security. An "insider," or a person with access to information pertaining to national security, may intentionally or unintentionally do harm to the security of the United States. This can be a witting or unwitting threat and may cause damage to the United States resulting from espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

As the information age gives way to the network age, competition is being defined and decided by interconnected human and technical networks. ARLIS believes an appropriate balance will require moving from an insider threat mentality, which is focused on finding individual "bad actors," to a paradigm of modeling and mitigating insider risk (MInR), which seeks to assign quantitative risks to a range of potential insider failure modes that can result in significant costs and damage to the organization.

Risk must be viewed as a function of threat, vulnerability, consequence, and time. The paradigm shift reframes the workforce as not only the source of threats but principally as part of the team that works to reduce risk by lowering individual and organization vulnerabilities to potential threats. The application of this risk equation and its variables will facilitate a less disruptive path to modeling and mitigating risk.

Risk must be viewed as a function of threat, vulnerability, consequence, and time.

In order to shift paradigms from determining and deterring insider threat to modeling and mitigating insider risk, the way that we think about threat and risk must be addressed. Using language that encourages problem-solving rather than defensiveness supports a stronger understanding of the problem. In doing so, measures taken to reduce or

eliminate insider threat or risk are moved from individuals and specific behaviors to long-term patterns and contexts.

LINES OF EFFORT

ARLIS has incorporated and explicitly embraced three key lines of effort that will be required for tackling Insider Threat, complementing it with an ability to model and mitigate Insider Risk.

Thinking differently

ARLIS is working to establish a scientific foundation—grounded in operational context—for modeling and mitigating insider risk, by way of mission-driven convening activities, integrating research across disciplines, and conducting new research. Efforts range from fundamental research on identity and "self" in the context of social media to building a lexicon to assist in DoD vetting of candidate International Military Students.

Operational test and evaluation

A wide range of existing and nascent technologies claim to address some dimension of insider threat. The government not only needs new knowledge and methods for MInR, but also ways to test, evaluate, verify, and validate (TEV&V) proposed approaches and tools.

In 2021 ARLIS conducted independent TEV&V and—to enable and encourage intentional and thoughtful innovation—also proposed an Evidence Readiness Levels framework (see figure), applicable for the insider risk domain and many other social science challenge areas in which it is more difficult to define and evaluate explicit measurement criteria (e.g., psychology, political science).

11	Operational use, with monitoring and evaluation
10	Target environment, at-scale operational evaluation, with independent expert review
9	Evaluate generalizability
8	Replicate and expand on ERL 7, across relevant factors, with independent expert review
7	Level II TOP, large scale, target-like controlled study, with independent expert review
6	ERL 5 replication, with independent expert review
5	Level II TOP, small-scale controlled study, with independent expert review
4	Case studies/anecdotal observations/ proof-of-concept
3	Potential solution developed
2	Finding or effect identified in literature, evaluate empirical support
1	Problem or finding observed

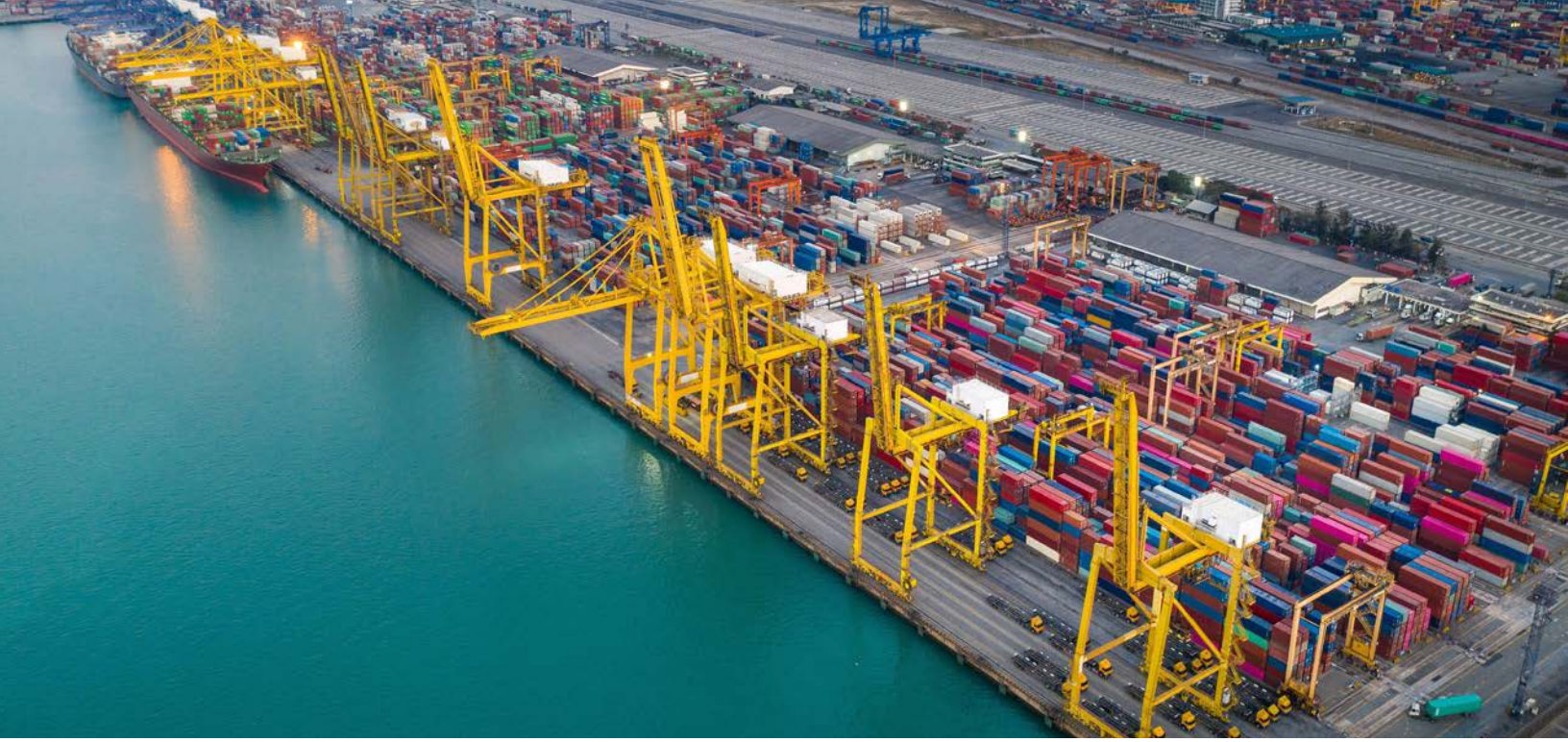
The ARLIS-proposed Evidence Readiness Levels (ERL) framework. "TOP" references Open Science Framework (OSF) Transparency and Openness Promotion guidelines.

Education and outreach

ARLIS draws upon its relationships with campus research partners and USG-internal training entities to make ARLIS the source for training and convening regarding Insider Risk. A 2021 pilot course has a likely sponsor for future rounds, and ARLIS anticipates its popular Insider RIsk Speaker Series attended by hundreds across the U.S for six months in 2021 will again serve as the glue that pulls together the Security Enterprise periodically for a fruitful discussion on Insider Risk. Education and outreach will bring together a strong, unified understanding of insider threat and insider risk and connect ARLIS to outside organizations and experts working in the mission space as well.

CHALLENGES AHEAD

Insider threat and insider risk are far-reaching, and ARLIS is working to reduce such harm to the United States. ARLIS has the unique opportunity to utilize its skilled personnel and campus resources to work toward modeling and mitigating insider risk, from research and development to new testing frameworks and education efforts. The research and outcomes described here will support not only immediate operational impact today but future impact on how things might be done tomorrow.



Acquisition and Industrial Security

The The Acquisition and Industrial Security mission area at ARLIS works to ensure the protection and safety of any acquired item, such as systems, data, operational technology, or products, and that they are delivered securely and uncompromised. Researchers identify what supply chains are most critical to the United States Government, and act as the integrator to solve problems across defense industrial space.

Everything is a supply chain. As a UARC, ARLIS has the unique ability to connect the components of supply chains—people, technology, organizational policy—to develop a comprehensive view to measure and control supply chain operations and the lifecycle of a supply chain. The teams in the mission area—composed of social scientists, engineers, computer scientists, and lawyers, among others—bring a sociotechnical perspective to understanding supply chains and to understanding criticality. They can look at this problem at the intersection of software, hardware, data, people, and processes.

ARLIS is building a supply chain-centered mission area and is an advocate for conceptual interoperability. That is, creating a common conceptual model of how supply chains work would create a foundation for a better understanding of and working ability for those working with supply chain operations. Further, the team is developing better understanding in the language of engineering and information science through the development of domain-specific data definitions that will enable new linguistics for navigating idiomatic idiosyncrasies of supply chain:

ARLIS approaches this challenge to understanding supply chain operations with three areas of focus.

- **Digital engineering**, identifying and solving security risks by better understanding the structure and connection of links across systems;
- **Operational technology**, creating an effective metric and measurement approach to continually monitor and validate the machine tools, factories, and industrial spaces in use ; and
- **Operational control**, studying the command and control of supply chains and production systems and identifying the needs in measuring and monitoring supply chains to enable trustworthy supply

CURRENT ACTIVITIES

Current activities at ARLIS largely serve to catalog, compose, and assemble agile, multi-functional networks of partners, capabilities, and information systems to tackle

real-time supply-chain and technology threats. Further, ARLIS acts as a trusted agent, subject-matter expert, and liaison between the IC and suppliers across various supply chains, which reduces barriers to information sharing and openness between the IC and suppliers.

Supply Chain Digital Twin

ARLIS's core funding in this mission area has supported creating cyberphysical systems, allowing the instrumentation and simulation of things in the real world. Specifically, ARLIS has been developing a modular, scalable digital twin framework that provides the ability to start a new modeling simulation environment at the push of a button. More than a modeling and simulation tool, it is an integration platform that combines data, analyses, and viewpoints, delivering the capability to perform data- and hypothesis-driven experimentation. This allows ARLIS to model simulations of supply chains for its clients and partners to determine and analyze the state of security and the risks that are brought over time in supply chain operations. The digital twin framework will also enable reusable tools and a redeployable template.

Illumination and Risk Evaluation

2020 Congressional language directed DoD to "develop an analytical framework for risk mitigation across the acquisition process." Reviewing the major "supply chain due diligence" commercial companies currently available, ARLIS researchers found none that could generate a holistic counterintelligence (CI) and security risk assessment of entities within, capturing key information and addressing strengths and weaknesses.

In response, ARLIS developed a methodology and scoring capability including analysis incorporating the major dynamic and interdependent business, CI, and security risks facing part of the Defense Industrial Base (DIB). These innovations, along with risk mitigation recommendations, will carry forward to scale-up to the entire DIB, not only meeting Congressional requirements but doing so in a way that will continue to evolve as the adversary adapts their tactics.

Protecting the Digital Engineering Mission

The DoD wants to pursue digital engineering (DE) to help speed the acquisition process and cut long-term sustainment costs. DE could also enable decision superiority in areas of strategic competition by enabling faster sensemaking of risks and courses of action.

ARLIS is meeting the changing demands of operational environments with DE solutions that enable the engineering of resilient, uncompromisable systems through decision superiority through the use of modeling, simulation, and tradespace analysis.

5G/Network Ventures

ARLIS is building off A&IS insights and leveraging expertise in wireless communications and cybersecurity to combine commercial technologies with custom DoD solutions, enabling the U.S. to operate through untrusted networks.

ARLIS is collaborating with both government and industry to devise a framework for identifying gaps where DoD needs to invest beyond protections implemented by commercial vendors and operators to meet unique DoD operational security needs. ARLIS is also creating a test facility for in-depth analysis and experimentation with emerging 5G capabilities and security concerns, including construction of a radio frequency-shielded enclosure for over-the-air testing and an open-source network-software test bed.

ARLIS-led T&E of 5G commercial hardware and software assesses security solutions and examines vulnerabilities. The technologies will include both those developed by commercial telecommunications-equipment providers as well as commodity hardware for hosting open-source software implementations of 5G protocols. For this latter work, ARLIS is teaming with INSURE member Morgan State University to investigate the Internet of Things vulnerabilities and mitigation.

> "DoD must make better use of its existing resources to identify, protect, detect, respond to, and recover from network and supply chain threat."
>
> – *DELIVER UNCOMPROMISED: A STRATEGY FOR SUPPLY CHAIN SECURITY AND RESILIENCE* FROM 2018 REPORT FROM THE MITRE CORP.

AI, Autonomy, and Augmentation

While the international research community continues to report tremendous progress in the development of Artificial Intelligence (AI), Autonomy, and Augmentation (AAA) technologies, the operational benefits of AAA technologies within DoD and IC have yet to be fully realized. As a trusted agent to DoD and IC, ARLIS applies its core competencies in sociotechnical systems developing human-centered approaches to incorporating AAA technologies that are trusted, reliable, and safe into operational workflows.

OPERATIONALIZING AAA

In 2021 ARLIS continued to tackle the challenge of operationalizing AAA technologies on multiple fronts: trusted test and evaluation, human-system integration, and foundational AAA research and development (R&D) in support of the first two categories. Trusted support work at the traditional systems engineering level has included test and evaluation of integrated systems against curated data and scenarios. In our mission of human-centered analysis and evaluation of technology, we have been working with government sponsors to perform workflow analysis and mission modeling to evaluate human-machine teams. Finally, ARLIS is performing R&D to enable the operationalization of AAA. This includes mission-focused prototyping, simulation-based verification to support test, evaluation, verification, and validation (TEV&V) for artificial intelligence and autonomy, and human-machine teaming.

AI Engineering Initiative

ARLIS is leading the Office of the Director of National Intelligence's (ODNI) AI Engineering initiative in partnership with Carnegie Mellon University's Software Engineering Institute. As part of this effort, ARLIS is developing concepts for community infrastructure as well as conducting research and development to advance and mature the AI engineering discipline. Additionally, ARLIS leverages its Research for Intelligence and Security Challenges (RISC) internship program to incentivize students to introduce students to key AI engineering and operations challenges with an IC context, supporting the pipeline of scientists, researchers, and engineers vital to ARLIS operations.

Project Maven

Project Maven (officially the Algorithmic Warfare Cross-Functional Team (AWCFT)) was established to accelerate the integration of best-of-breed AI technologies into DoD. ARLIS is conducting T&E on the Collected Exploitable Materials line of effort, focusing on ensuring excellence in the data processing pipelines the sponsor is developing for Natural

Language Processing—identifying events and named entities of interest.

Project Gargoyle

ARLIS continues its development of novel methodologies for operational test and evaluation of AI technologies with Project Gargoyle. This project is an effort to embed cutting-edge machine learning and artificial intelligence capabilities in existing defense systems. ARLIS is working with the USG to assess the efficiency and performance of Full Motion Video operators and workflows integrating computer vision capabilities within existing surveillance systems.

Artificial Intelligence and Autonomy for Multi-Agent Systems (ArtIAMAS)

In May 2021, the University of Maryland was selected to lead a five-year, $65M cooperative agreement with the Army Research Laboratory known as ArtIAMAS—Artificial Intelligence and Autonomy for Multi-Agent Systems. ARLIS is a critical partner in this campus-based effort, leading three fundamental research projects:

- Human-Machine Teaming and Effective Aggregation of Information in Complex Systems,
- Simulation-Based Verification and Validation for Autonomous Systems, and
- Conceptualizing and Assessing AI Technological Fluency.

Human-Computer Interaction

ARLIS's Human–Computer Interaction Laboratory was established in 2021 with portable and reconfigurable capabilities, such as software instrumentation for behavioral workflow, task analysis, and integrated psycho-physiological analysis (tethered and untethered) in the areas of electrocardiography, electromyography, respiration, electrodermal activity, and eye tracking.

With both unclassified and classified instantiations, ARLIS's mirrored data collection and user-testing capabilities allow researchers to benefit from replication and efficiencies generated in unclassified use-cases.

AUGMENTING COLLECTIVE INTELLIGENCE

To maintain strategic advantage over those who seek to undermine the security of democratic systems and nations, the USG seeks to better leverage a powerful and unique advantage: our workforce. Our people bring an unparalleled diversity of experiences, skills, abilities, perspectives, and insights which, if leveraged appropriately, can enable rapid

identification and response to new threats. Adversaries who enforce a strongly hierarchical or top-down governing structure or who over-rely on the promise of artificial intelligence to inform decisions, do not have this opportunity. Diversity is an asymmetric advantage for democracy.

Crowdsourced forecasting enables access to the collective wisdom of our diverse workforce. The scientific underpinnings and methodology have been proven across multiple scientific research programs, and government and private sector adoption. Building on this foundation, ARLIS is introducing INFER—the INtegrated Forecasts and Estimates of Risks crowdsourced forecasting platform—to tap the collective intelligence of the USG workforce at scale and provide decision-makers with consensus probabilistic forecasts that inform policy. Initial topics, in support of research and development objectives to inform policy and decision making, include forecasting science and technology trends.

Beyond forecast accuracy, INFER will bring other benefits to USG.

- **Clarity**: quantitative forecasts that move away from ambiguous, easily misinterpreted verbiage such as "likely" or "highly unlikely"
- **Speed**: crowds that can generate initial forecasts in hours rather than weeks or months
- **Track Record**: trajectories of forecasts over time that provide valuable lessons learned
- **Focus**: a forecasting skill distinct from domain expertise, fitting for today's missions

The targeted launch for INFER is Spring 2022, as an unclassified platform restricted to .mil, .gov, and other official accounts. In addition, ARLIS will operate a second platform that will be fully open to contractors, think tanks, universities, and the like, in order to benefit from non-USG and international partner forecasters.

Human Language and Culture

ARLIS's origins as a UARC were focused on comprehensive language preparedness for DoD and the IC, particularly in the aftermath of the September 11 terrorist attacks. Then known as the Center for Advanced Study of Language (CASL), the organization assembled a stronghold of top-quality language, culture, and human performance researchers capable of responding to immediate operational requirements while still pursuing the strategic research needs of the government.

Due in part to this history, language research has always been a critical enabler for ARLIS mission areas, including cognitive security, insider risk, performance augmentation, and other problem spaces where data remains unstructured, multilingual, or derived from social media. Beyond work in human language technologies, linguists and language experts are directly involved in many of ARLIS's current projects in other mission areas, along with the direct generation of high-quality data resources for government and research communities at large.

ARLIS's language and culture researchers are particularly active in performing test and evaluation for funding agencies. Much of this work involves the collection, curation, and annotation of data in numerous mission-critical languages, including low-resource languages. These gold-standard datasets are then used in the development of human language technologies that can be used to assist analysts in triage, translation, and/or analysis of foreign language text and speech.

ARLIS has a separate vein of research to better understand messaging and influence across different languages and cultures. This includes developing a better understanding of the role of emotions in communication, how emotions may be expressed differently in different languages and cultures, and the role that emotions play in online social media sharing behaviors. ARLIS also serves as the T&E partner on a program that works to detect influence campaigns. In this capacity, ARLIS develops scenarios, evaluation metrics, and annotated datasets to inform the program's understanding of the role of agendas, concerns, and emotions in influence campaigns.

ARLIS researchers bring deep expertise in languages and cultures across the globe (see page 21 for figure). When

The layer of human understanding from ARLIS language and culture experts gives its research depth of meaning and cultural significance in navigating relations and perspectives surrounding international affairs.

additional language expertise is needed, we leverage our networks and partnerships internationally to rapidly bring in expertise as required, such as for building data resources for the government and research communities.

SENTIMENT DETECTION TO ASSESS INFLUENCE FROM CHINA'S BELT AND ROAD INITIATIVE

Given its strengths in diverse languages and linguistic analysis, ARLIS uniquely tackles problems that require understanding of non-English languages and scripts. An example of this is ARLIS's research into the Belt and Road Initiative (BRI) investment projects in Kenya, seeking to understand whether indicators of Chinese influence could be revealed through automatic and manual text analysis of local language social media communications.

Researchers examined a key gap in influence and information operations: the ability to see and understand how sentiment will change in a given area based on changes in messaging and current events. Specifically, the project looked at attitudes and sentiments of Kenyans in the context of Chinese BRI investments that have taken place in Kenya over the last eight years. Local reactions to these projects range from addressing personal impact and experiences to political commentary and persuasion efforts. Expertise in cross-cultural communications and natural language processing allowed ARLIS to apply both manual and automated techniques for English- and Swahili-language social media alongside conventional regional news media, to collect and analyze data surrounding questions of attitudes of Kenyan citizens toward the BRI projects and Chinese involvement.

The collected data indicated that attitudes of Kenyan citizens towards specific infrastructure projects in Kenya were generally positive; however, attitudes towards China's role in Kenyan infrastructure development skewed more negative and were predominated by debt concerns. Discussion of BRI projects was strongly intertwined with discussion of corruption at the national or local level. Other findings included the identification of specific communication practices that emerge in multilingual social media communities, such as social media posts written in Swahili but using English hashtags.

Leveraging language expertise to further cognitive security research, ARLIS looked at attitudes and sentiments of Kenyans in the context of Chinese investments in Kenya over the last eight years.

Unique Foreign Language Expertise

ARLIS capabilities includes deep expertise in languages and cultures across the globe (pins). Diamond shapes indicate data resources built by ARLIS by rapidly drawing expertise from the broader language community.

Strengthening the Workforce

RESEARCH FOR INTELLIGENCE & SECURITY CHALLENGES INTERNSHIP PROGRAM

ARLIS successfully executed the 2021 Research for Intelligence and Security Challenges (RISC) Initiative summer internship program, marking a year of growth and expansion over the 2020 inaugural program.

The goal of the RISC Initiative is to create and nurture a pipeline of student talent at both the graduate and undergraduate levels, providing an understanding of the security and intelligence community's technical challenges and the career opportunities that exist to work on them. Over an intensive 10-week program, competitively selected interns were paired with mentors from the UMD faculty and government experts from the national security community. They worked in teams, gaining hands-on experience analyzing, designing, and engineering solutions for existing real-world DoD and IC issues.

The program was structured to facilitate interaction between participants. Student teams presented research updates to their intern peers for critical feedback at regular RISC Roundups and developed final reports as a deliverable in tandem with a sharable code base and, in some cases, policy recommendations briefed to government audiences as well. The RISC Program concluded with a workshop and demonstration event, each team briefing a panel of IC/DOD experts and leadership.

The 2021 RISC Program expanded its scope as it entered its second year. In 2020 the AIRICC summer internship focused on technical challenges in the Artificial Intelligence and Machine Learning fields, with the National Geospatial-Intelligence Agency (NGA) as its sole sponsor. The successes from 2020 inspired project sponsorship from two additional government agencies (the Office of the Director of National Intelligence (ODNI) and the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). The project list below demonstrates the topical breadth of the fourteen real-world intelligence and security problems, posed by government operators and supported with realistic data sets.

The 2021 RISC Program also expanded its outreach. Interest increased from 27 applications in 2020 to 105 applications in 2021, and 38 interns were selected (versus 17 in 2020). The participating 28 undergraduates and 10 graduate students came from 12 universities across the INSURE consortium and beyond.

In the year ahead, ARLIS anticipates another doubling in size and further expansion of sponsorship and scope, engaging top undergraduate and graduate students interested in supporting intelligence and security research and development.

2021 RISC INTERNSHIP PROJECT TITLES

National Geospatial-Intelligence Agency Projects
- Improving Solid 3D Modeling from Point Clouds
- Algorithms for Threat Detection
- Open-source research to support permafrost mapping

Defense Intelligence & Security Projects
- Framework to Transform DoD Declassification
- Security Enterprise Oversight Metrics
- Evaluating and Optimizing Security Training
- Strategic Messaging Effects

Office of the Director of National Intelligence Projects
- Implicit Structure from Explicit Format
- Threats and Opportunities of Open-Source AI/ML for the IC
- Analyzing Water Sector Vulnerabilities and Securing SCADA Systems

ARLIS Research Topics
- Assessment & Evaluation of Defense Applications for Emerging AI Hardware
- Adversary Perceptions of US Response to the COVID-19 Pandemic
- Cognitive Security Social Media Simulation
- Defining Insider TRUST (Trustworthy, Reliable, and Useable Systems and Teams)
- Crowdsource Forecasting for Modeling Insider Risk (CSIFT for MInR)

TECHNOLOGY AND LAW ACADEMY

The Technology and Law Academy (TLA), in partnership with UMD ARLIS, brings together academics, lawyers, and technologists to learn and practice technology law and effectively address legal and operational challenges presented by new technologies. The six-week courses presented by the TLA immerse small groups of academics, professionals, and practitioners in the substantive and legal dimensions of the most critical technologies in the national security realm, including cybersecurity, AI and machine learning, telecommunications, internet exploitation, and space.

The TLA has run two courses in technology law and acquisition since 2020. During the spring 2021 semester, the Defense Intelligence Agency (DIA) and UMD ARLIS presented a new six-week course in technology acquisition.

Acquiring Emerging Technologies Course

The *Acquiring Emerging Technologies* (AET) course—held in a combination of virtual and in-person methods—explored innovative ways to acquire emerging technologies that enhance the Intelligence Community's (IC) collection capabilities and the timely delivery of fact-based, well-reasoned judgments to warfighters and policymakers. Such understanding mitigates and prevents delays in technology acquisition otherwise faced during the challenging processes of staffing and acquisition. The focus of AET was to meet a gap in intelligence needs by addressing such delays with innovative approaches and strategies.

Upon completing this course, students were expected to have:

- Advanced knowledge and skills they can use to solve complex problems in the acquisition of emerging technologies in the IC,
- A sophisticated understanding of how emerging technologies help the IC in filing intelligence requirements and deliver analysis to the warfighters and policymakers in a timely manner,
- Mastered innovative ways to address the acquisition of emerging technologies under current FAR and non-FAR authorities and processes, and
- Broadened their professional network.

This course enabled senior intelligence, legal, and/or contracting professionals to understand, discover, and develop innovative acquisition strategies for emerging technologies that provide for timely analysis of raw data to provide intelligence products for decision makers, policymakers, and the warfighter at the speed of mission.

> "The fundamentals of what an intelligence professional is and does is likely to change dramatically. Current officers will be required to prepare for a tech-driven future while still mastering present-day missions and tasks."
>
> – *MAINTAINING THE INTELLIGENCE EDGE*, 2011 REPORT FROM THE CENTER FOR STRATEGIC INTERNATIONAL STUDIES

RISC interns and ARLIS researchers greet Testudo the Turtle at the ARLIS summer team building event.

Partnerships in Higher Education

STRENGTHENING THE INTELLIGENCE AND SECURITY UNIVERSITY RESEARCH ENTERPRISE

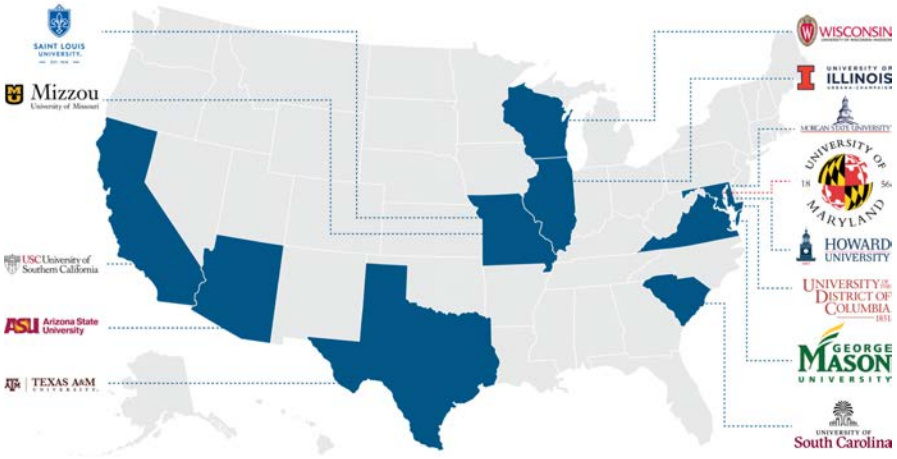
Building teams to support government sponsors on their most critical sociotechnical challenges requires ARLIS to be agile and creative. ARLIS stood up the Intelligence and Security University Research Enterprise (INSURE)—a consortium of trusted university partners working together to respond to difficult intelligence and security problems—to help it:

1. Bring the right team to every problem ARLIS supports as a UARC,
2. Be the connector and translator for the IC and defense security communities to engage university talent (and for university researchers to more effectively target their efforts to the benefit of those communities), and
3. Combine resources to strengthen the current IC/DSE workforce and build a robust and diverse future workforce. Priorities include inventorying and sharing I&S-relevant professional education programs, STEAM initiatives, and working to bring new talent into the field.

INSURE members include notable Carnegie-R1 research institutions alongside quality top institutions too often left out of applied defense research such as Historically Black Colleges and Universities (HBCUs) and other minority-serving institutions. All bring institutional strengths in ARLIS priority areas, a track record conducting applied, quick-turn, mission-relevant R&D, existing relevant security partnerships to integrate into INSURE stakeholder community, and institutional leadership buy-in, to ensure sustained partnership not reliant on individual researchers or projects.

INSURE projects are within scope of ARLIS core competencies and of UARC character. They include an ARLIS lead to track progress, connect relevant stakeholders, and integrate the effort into the corresponding ARLIS portfolio. There are multiple pathways to funding, including a member(s) engaging a potential sponsor directly about work and develop programming, members conducting joint program development, leveraging inter-institutional strengths, or a USG agency requests R&D effort needing ARLIS partners' strengths.

2021 saw rapid expansion, process development, and regular technical exchanges to build interconnectivity and robust sponsor relationships. In the year ahead, INSURE will continue its work tapping top talent across the network to support a range of security and intelligence stakeholders while also pushing forward high visibility initiatives in a select set of challenge areas where ARLIS and INSURE are uniquely positioned to make outsized impact as a research enterprise.



> "No matter who you are, most of the smartest people work for someone else."
>
> – BILL JOY, FOUNDER OF SUN MICROSYSTEMS

2021 External Advisory Board

The ARLIS External Advisory Board members lend their expertise to steer the broad research and impact goals of ARLIS. These advisors, from a range of disciplines and backgrounds, are leaders in government, corporate, and academic arenas.

Prof. David Bader (UMD Ph.D. 1996) is Distinguished Professor in the Department of Computer Science and Director of the Institute for Data Science at New Jersey Institute of Technology.

Dr. Steve Cambone is Associate Vice Chancellor for Cybersecurity Initiatives for the Texas A&M University System and previously served as the first Under Secretary of Defense for Intelligence, a post created in March 2003.

LTG (Ret.) Edward Cardon is a Professor of the Practice at UMD and formerly served in roles including Commanding General, U.S. Army Cyber Command, and Director, Office of Business Transformation, leading the Task Force that helped create Army Futures Command. ***[ex-officio]***

Lt. Gen. (Ret.) **James Clapper** is a retired lieutenant general in the United States Air Force and is the former Director of National Intelligence and former Under Secretary of Defense for Intelligence, among other roles.

Prof. Rita Colwell is Distinguished University Professor at UMD, a member of the National Academy of Sciences, and a former director of the National Science Foundation.

Dr. Steve Fetter is Associate Provost and Dean of the Graduate School, University of Maryland and former leadership within the White House Office of Science and Technology Policy.

Dr. Gary Flake (UMD Ph.D. 1994) is a technology advisor, investor, and inventor, with past technical leadership roles at Salesforce and Microsoft and as the founder of Yahoo! Research Labs.

Vice Admiral (Ret.) Paul Golden Gaffney II was the seventh president of Monmouth University in West Long Branch, New Jersey, from 2003 to 2013, becoming president emeritus August 1, 2013. Gaffney graduated from the United States Naval Academy in 1968. He is the former Chief of Naval Research.

Dr. Robert Kahn is the founder and CEO of the Corporation for National Research Initiatives (CNRI). Among other technical achievements, Dr. Kahn was responsible for the system design of the Arpanet and originated DARPA's Internet Program.

Ms. Letitia Long is Chairman of the Board of the Intelligence and National Security Alliance and former Director of the National Geospatial-Intelligence Agency—the first woman to lead a major U.S. intelligence agency.

Mr. Gilman Louie is a partner at Alsop Louie Partners and is the founder and former CEO of In-Q-Tel, an independent, non-profit venture capital firm established with the backing of the Central Intelligence Agency. Mr. Louie is also a commissioner to the National Security Commission on Artificial Intelligence and Chairman of the Federation of American Scientists.

Adm. (Ret.) William Moran is the former Vice Chief of Naval Operations, with previous roles as the Chief of Naval Personnel and Deputy Chief of Naval Operations for Manpower, Personnel, Training, and Education.

Dr. Eliahu Niewood is Vice President of the Intelligence Center and Cross-Cutting Capabilities at MITRE.

Dr. Alton Romig is the Executive Officer of the National Academy of Engineering and former VP & GM of the Lockheed Martin Aeronautics Company Advanced Development Programs (i.e. Skunk Works) and Deputy Lab Director of Sandia National Laboratories.

Maj. Gen. (Ret.) Annette Sobel is Associate Professor in Medical Education and Biomedical Sciences at Texas Tech University and an expert in human factors research. Past roles include senior advisor for biological defense for the Defense Threat Reduction Agency and Office of the Secretary of Defense.

Lt. Gen. (Ret.) Vince Stewart, USMC, is Chief Innovation and Business Intelligence Officer for Ankura, former Deputy Commander, U.S. Cyber Command, and former Director, Defense Intelligence Agency.

Adm (Ret) William Studeman is a retired admiral of the United States Navy and former deputy director of the Central Intelligence Agency—with two extended periods as acting Director of Central Intelligence—and former director of the National Security Agency.

Dr. Michael Vickers is a former Under Secretary of Defense for Intelligence. He previously served as Assistant Secretary of Defense for Special Operations, Low-Intensity Conflict, and Interdependent Capabilities, as a CIA Operations Officer, and as an Army Special Forces Officer.

Prof. Ellen Williams is Distinguished University Professor and Director of the Earth System Science Interdisciplinary Center at UMD and Chair of the JASONs. Her past experience includes serving as Director of the Advanced Research Projects Agency for Energy (ARPA-E).

Financial Overview

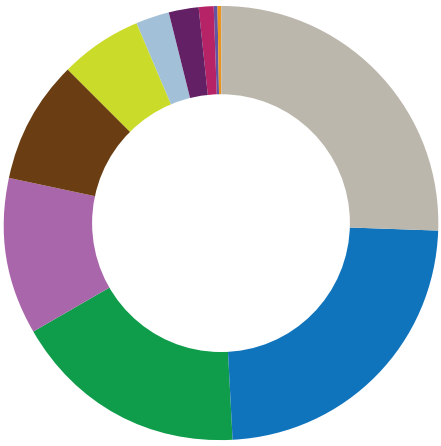
The growth in new awards and expenditures seen in government fiscal year (GFY) 2019 and 2020 continued into GFY 2021. During the fiscal year that ended September 30, 2021, ARLIS earned additional revenue from awards and contracts, totaling $46 million. As a nonprofit University Affiliated Research Center, the revenue that we earn is invested in our research and development endeavors, our facilities, and educational programs.

The figures below illustrate the distribution of the $46 million in new awards made in GFY 2021, in terms of mission focus, sponsor, and project type. Computational infrastructure is listed as a mission area but more accurately reflects focused investments being made in upgrading technology and data infrastructure in support of the other mission areas.

Award Dollars Across Mission Areas
USD FY21

- Acquisition & Industrial Security
- AI, Autonomy, and Augmentation
- Cognitive Security
- Collective Intelligence
- Resource Building
- Workforce Programs
- Other Research & Services

Sponsorship Profile
USG FY21



- Air Force
- Army
- Intelligence Community
- DARPA
- Industry
- Navy
- OSD Strategic Capabilities Office
- OUSD for Intelligence and Security
- OUSD for Research & Engineering
- U.S. Special Operations Command
- Private Philanthropy

Project Types
USG FY21

- Consortium
- OUSD I&S (core sponsor)
- RDT&E for others
- Trusted Agent

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

7005 52nd Avenue, College Park, MD 20742 | 301-226-8900 | info@arlis.umd.edu | www.arlis.umd.edu