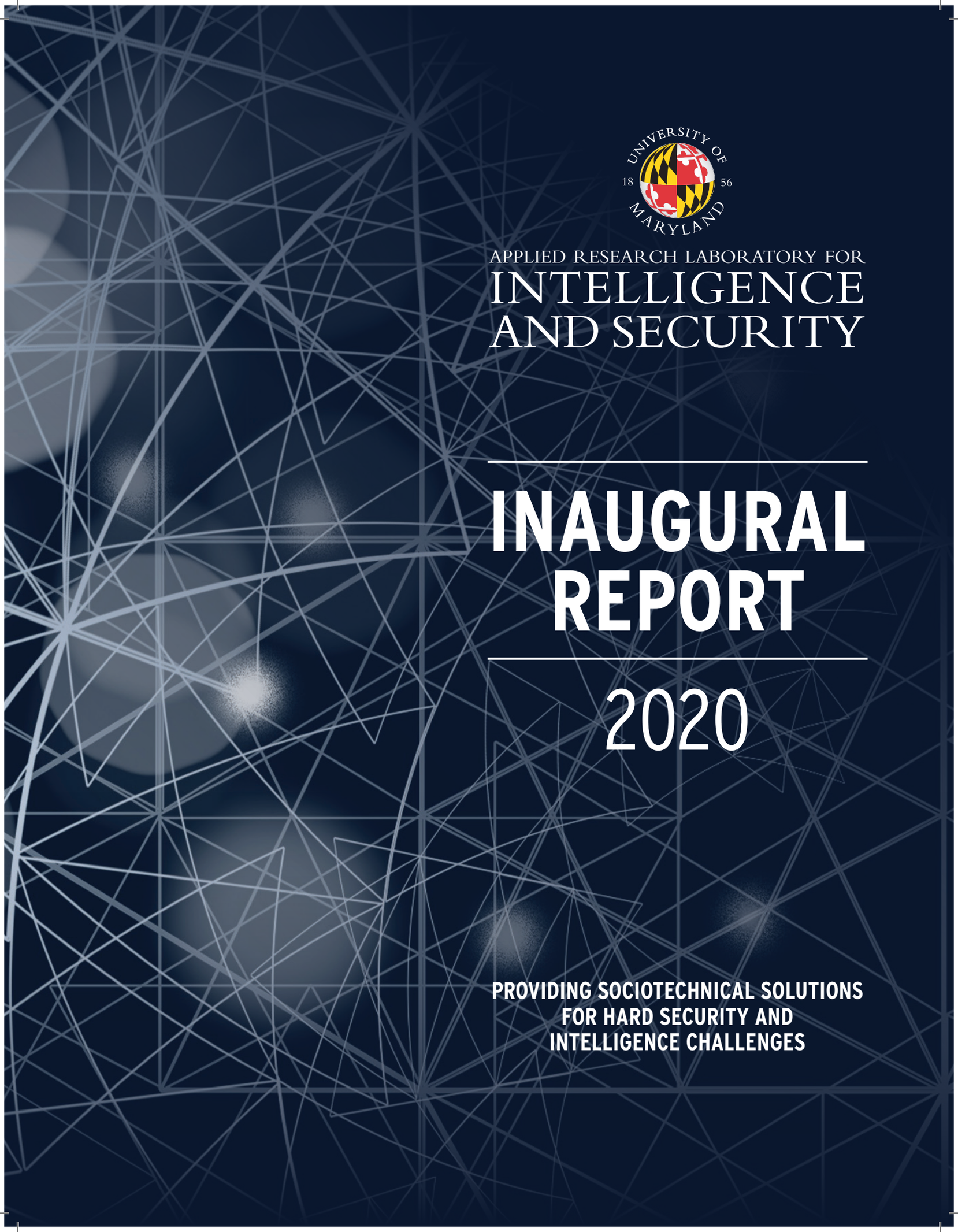


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

INAUGURAL REPORT

2020

PROVIDING SOCIOTECHNICAL SOLUTIONS FOR HARD SECURITY AND INTELLIGENCE CHALLENGES

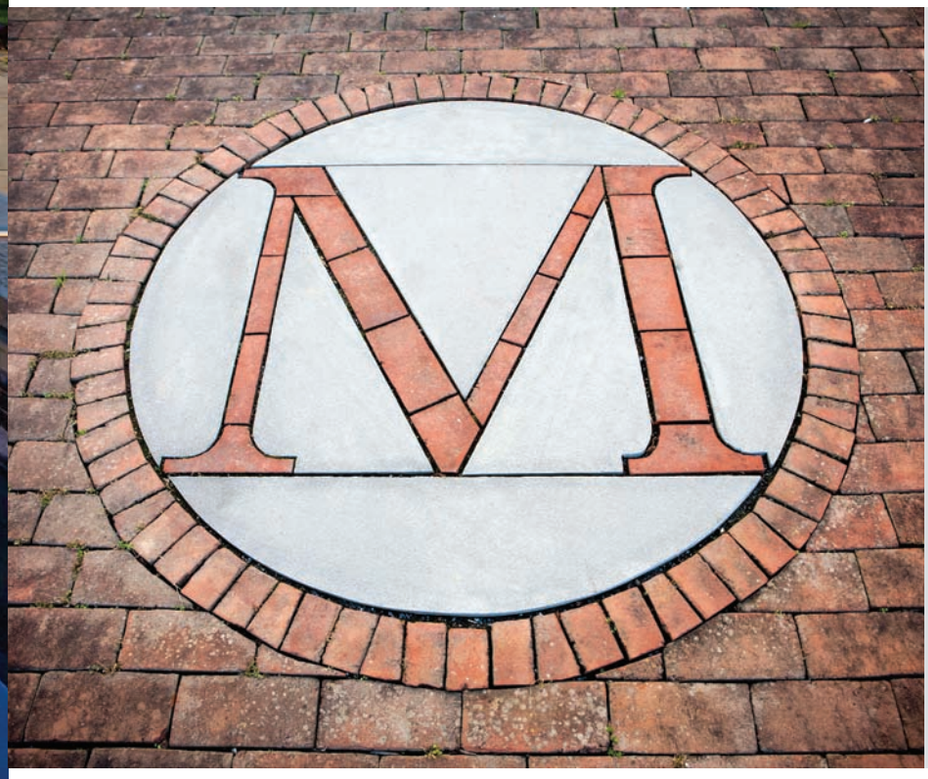
Welcome

A MESSAGE FROM THE EXECUTIVE DIRECTOR

The first annual report for the University of Maryland's Applied Research Laboratory for Intelligence and Security (ARLIS) represents the cumulation of a transition for one of the Department of Defense's University Affiliated Research Centers. Working with the Office of the Under Secretary of Defense for Intelligence and Security and national security stakeholders from across the government, the ARLIS team has created the foundations for an adaptable science and technology organization with unique strengths in areas increasingly recognized as critical for security, including social science, culture and language, and the applications of computation, data, and artificial intelligence to the challenges of the Intelligence and Security communities.

Presented in this report is a sampling of a cross-section of the ARLIS project portfolio as well as some of the accomplishments of our cohort of scientists and engineers addressing national security problems that range from modeling trust among people and systems, understanding influence and emotional content of social media, and developing more effective human-machine teams. Also described are a number of nascent programmatic efforts as ARLIS develops training programs and builds a university consortium to further serve the UARC mission. This report marks an important transition point for ARLIS. In the coming months and years, we look forward to working with our government stakeholders and university partners to agilely deliver new understanding and new approaches leveraging our core competencies, enhancing our national decision-makers' capabilities for tackling new and enduring problems in the Human Domain.

Dr. William Regli
Executive Director
University of Maryland, Applied Research Laboratory for Intelligence and Security (ARLIS)



CONTENTS

Who We Are

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 artificial intelligence, information engineering, and human systems. One of only 14 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 U.S. Government as an independent and objective trusted agent.

Critical to generating robust analysis and trusted tools in the human domain is the ability to pull together with true multi-disciplinary 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. Our renowned research team draws from a wide range of diverse expertise and disciplines, including engineering, data science, psychology, computer science, anthropology, rhetoric, cognitive science, political science, cyber security, linguistics, and machine-learning and artificial intelligence. 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.

A LOOK BACK AT FY 2020 PRIORITIES

Though a traditional "annual report" focuses on outputs from the previous year, the ARLIS Inaugural Report highlights not only accomplishments but also serves to present the organizational framework and targeted portfolio developed in the organization's first two years.

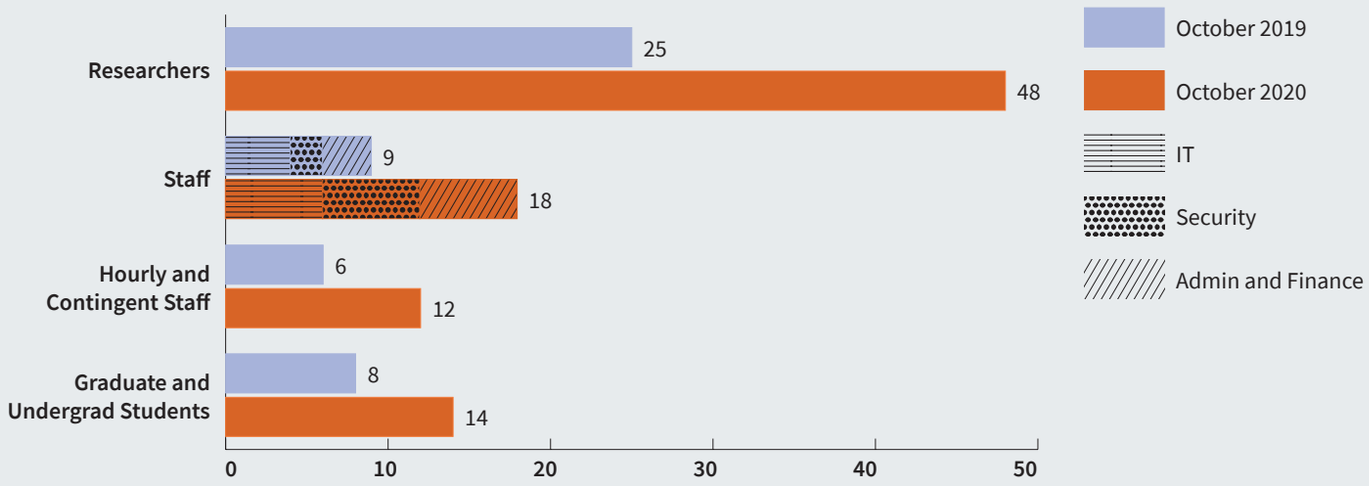
In fall 2019, going into Government Fiscal Year 2020, ARLIS had made significant progress in securing new sponsors and identifying initial problems important to our core sponsor OUSD(I&S) while leveraging existing strengths. That said, there was still work to be done to translate ideas into a cohesive strategic plan-making clear the unique value ARLIS would provide its customers. ARLIS priorities for FY 2020 included:

- Developing USG stakeholder community for ARLIS spanning the defense security and intelligence;
- Establishing a shared roadmap for OUSD(I&S) UARC activities and S&T activities;
- Identifying 2-3 core mission areas and technical capabilities broadly demanded by USG and appropriate for the ARLIS UARC to lead; and
- Building an adaptive staffing and partnership ecosystem to support current and future project execution.

ARLIS made notable progress across all four priority areas during the past year, resulting in the formation of a robust USG stakeholder community (e.g., with eight government agencies participating in the Spring 2020 ARLIS Program Review); a jointly developed strategic vision with core sponsor OUSD(I&S); the creation of a multi-university consortium reinforcing ARLIS mission; and solid technical progress and planning for the program areas highlighted in this document. In addition, FY 2020 included significant hiring of both technical talent and staff support (see figure on opposite page) and new programs to develop and curate the next generation of talent to tackle tomorrow's problems.

To help ensure that our work in this area reflects U.S. core values, principles, and respect for persons, ARLIS formed in 2020 an ELSI advisory board to provide guidance on the Ethical, Legal, and Societal Implications of considered and active research.

ARLIS GROWTH



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 skillsets – available to them to help address their needs and solve problems.

A key tenet of being a DoD-designated UARC[1] is for ARLIS to operate in the public interest as a strategic partner with our government sponsors, rather than in the interest of corporate shareholders, and to conduct its business in a manner befitting its special relationship with DoD, combining technical excellence with objectivity. ARLIS's role as a UARC enables a strategic relationship with our sponsors that gives it knowledge of its sponsors' needs and access to their information.

Across the six ARLIS mission areas described in this report, ARLIS researchers are working to better serve as an independent, trusted advisor supporting the government as a Test & Evaluation (T&E) partner, performing verification and validation, and broadly contributing to the government's mission as subject matter experts across a wide range of disciplines.

As the sole UARC primarily focused on the Intelligence and Security communities, UMD ARLIS is building relevant long-term capabilities for our government sponsors, applying multidisciplinary methods to solve the most challenging security problems facing the nation and worldwide. In this pursuit, ARLIS has been hiring aggressively and establishing new partnerships — to include the Intelligence and Security University Research Enterprise (INSURE) consortium described later in this report — to expand and deepen its bench of expertise available in service of our government customers.

FACILITY AND RESEARCH INFRASTRUCTURE

UMD ARLIS's 128,000 square-foot secure workspace provides our government partners with secure access to our mission-area capabilities and breakthrough scientific research. Our facility also features a 180-person auditorium and an 80-person large conference room, including secure video teleconferencing (VTC) for multi-participant meetings or forums at the classified level.

Conveniently located in the National Capital Region, ARLIS and our government and academic partners collaborate on events and projects for the DoD and IC communities throughout the year. Beyond facilitating classified work, our large facility has proven to be a uniquely advantageous venue for hosting conferences and wargaming exercises. In 2019 and 2020, with over 100 participants and distinguished guests present, this facility enabled ARLIS to support three high-visibility cyber resilience exercises not only technically but also as event host, with a multi-room real-time and adaptive game-play infrastructure in a classified environment.

[1] From: ***Engagement Guide Department of Defense University Affiliated Research Centers,*** April 2013.

Current Mission Areas

The information age has evolved into the network age, with the world increasingly being defined and shaped by interconnected human and technical networks. This is leading to new complexities as our physical, digital, and social selves merge within these "sociotechnical" networks, which are the hallmark of the Human Domain — the domain where tackling hard problems depends critically on understanding and designing systems for human strengths, limitations, vulnerabilities, and diversity.

These sociotechnical complexities present both new opportunities and new challenges for the U.S. and its allies, who face long-term competitions that increasingly occur within the Human Domain. Whether ensuring the cognitive security of democratic nations, protecting increasingly complex supply chains, addressing insider risk, projecting and certifying on-task performance for AI systems that are being inserted into human work processes and systems, or augmenting human-machine "collective intelligence" to enhance complex decision-making, assuring advantage in the Human Domain will require new approaches that can effectively combine "Computing, Code, Cognition, and Communities." Accordingly, ARLIS has been launched to be the "UARC Human Domain Integrator" with the vision of becoming a preeminent, trustworthy partner to the nation in building the bench and capabilities required to develop sociotechnical solutions for the most difficult national security Human Domain challenges our country faces today.

As a UARC, ARLIS serves the public interest as independent technical leaders with a clear purpose of building and maintaining a long-term, committed relationship with the DoD and its partners. Our mission is to help to ensure U.S. and allied decision-advantage in long-term Human Domain competitions, in part by leveraging our core competencies in social and behavioral sciences, data science and infrastructure, AI/machine-learning, engineering, and advanced computing. By developing solutions that effectively combine humans **and** technology, rather than focusing on humans **or** technology, ARLIS ultimately seeks to have a significant and positive impact on our lives, our communities, our nation, and the world.

The following pages detail the objectives and current ventures in six current mission areas, as framed in the figure below.

THE UARC FOR THE HUMAN DOMAIN

ASSURING US AND ALLIED ADVANTAGE IN THE HUMAN DOMAIN

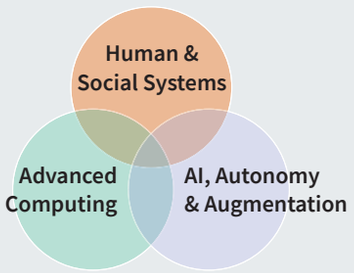
The Human Domain: where understanding and designing for human diversity—behaviors, beliefs, values, strengths, limitations, and vulnerabilities—confers competitive advantage in "Computing, Code, Cognition, and Communities"

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

Test and Evaluation

Ethical, Legal, Societal Implications Panel

SMEs on Call



University Consortium

Computational Infrastructure

Education and Training

Language & Culture as Research Enablers

Enabling Cognitive Security | Acquisition & Industrial Security | Modeling & Managing Insider Risk | Decision Support & Performance | Augmenting Collective Intelligence

Enabling Cognitive Security

Disinformation is one of the most critical issues of our time, concerned with online and offline influence at scales ranging from individuals to large societies. Operations in the Information Environment (OIE) are conducted within the context of **Cognitive Security**, or COGSEC.

Our adversaries, competitors, partners, and allies are all engaged in these activities, which are growing in scope and scale. Many of these concepts and techniques have multiple uses, so that research in marketing, advertising, social media, and political campaigns accelerates the pace of security research and applications. This multi-use acceleration further compounds the complexity, the creation, and expansion of information technologies. The movement toward symbiotic human-machine interfaces creates an urgent demand for research to inform operations in the broadest sense.

The ARLIS COGSEC program is developing both targeted projects and overarching capabilities ready to use for a broad range of research, wargaming, and operational questions, with goals including the following:

- **Design** online systems and interactions to reduce vulnerability to misinformation and manipulation;
- **Detect** and mitigate targeted information manipulation attempts targeted at governmental insiders; and
- **Develop** the integration of cyber and social media systems or simulations while also monitoring factors outside social media environments.

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 2020 ARLIS began its work building a Cognitive Security Proving Ground (CSPG) to address this gap.

The CSPG will be a comprehensive Live, Virtual, and Constructive (LVC) platform that integrates human subject experimentation, modeling and simulation, and datasets for information operation environments. Other capabilities will include:

- Controlled human experiments integrated with simulation-based testing to optimize experimental control, measurement capabilities, and realistic levels of system complexity;
- A secure test and evaluation environment;

- Addressing a broad range of strategic and tactical questions for research, wargaming, and operations; and
- Ultimately, promoting a single common operating picture via interoperability with other test and evaluation, command and control, and IC and DOD systems.

The Proving Ground will enhance our ability to research and engineer 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.

A CURRENT VENTURE: HOW EMOTIONS INFLUENCE

Adversarial entities around the globe continue to spread disinformation on social media and have revealed a severe vulnerability in the security of the United States and its Western allies. The ARLIS-led Emotions in Social Media research project (https://emotionsinsocialmedia.umd.edu) is funded through the prestigious DoD Minerva Research Initiative program to investigate the spread of information campaigns by examining how different emotions influence resharing content in Polish and Lithuanian socio-political social media.

ARLIS's multinational Minerva team is collecting and analyzing real-world Facebook and YouTube data from Poland and Lithuania — countries that were chosen for their strategic relevance to NATO and Europe. Researchers are annotating samples of over 1,000 public Facebook posts and 300 YouTube videos from each country for emotions and topic content. Our team is also conducting computational linguistic analyses from 2015 to 2020 to examine sociopolitical topics and cross-platform information spread.

Most importantly, the *Emotions in Social Media* project addresses critical gaps in research about how information spreads across social networks. If successful, researchers can enhance our understanding of how emotion can affect behavior online and what types of emotional content are most likely to make messages go viral, for good or ill.

Researchers are examining the role of emotion in helping online messages go viral. Included in the study is *kama muta (*Sanskrit for "moved by love"*),* which is a heart-warming emotion when viewing something endearing or cute.

Acquisition and Industrial Security

The expansion of global networks, decentralization of manufacturing systems, and lack of research connected to real production capabilities have exposed defense-critical supply chains to greater risks of disruption, malfunction, danger, and logistical anomalies.

ARLIS seeks to become the preeminent thought-leader in **Acquisition and Industrial Security (A&IS)**, using consequence-driven research and a holistic approach to identify and address critical needs for enabling our nation's supply chains to "deliver uncompromised"[2] critical capabilities for intelligence and security.

ARLIS performs applied research in illuminating and vetting supply chains while also testing and evaluating the security of various technology used to facilitate them, particularly 5G wireless. By leveraging our technical and social science core competencies to address sociotechnical problems, we protect supply chains and technology. The security community and defense industrial base (DIB) cannot effectively illuminate, secure, and manage the supply chain risk using only a technological approach. Rather, an integrated, macroergonomics approach that accounts for all aspects of the supply chain (e.g., people, organizations, systems, and technology) must be deployed.

ARLIS research and development in AI&S will expedite a response to supply-chain threats, development, and vetting of A&IS methods and technologies. As a UARC, ARLIS can be a trusted partner for U.S. government stakeholders and industry leaders, illuminating supply chains and risks by mastering a risk-based framework and designing revolutionary methods to monitor security.

SOME CURRENT VENTURES

ARLIS leverages a network of partners, capabilities, and information systems to solve real-time supply-chain and technology threats, leading a team of rapid responders including trusted agents, subject-matter experts, and liaises between the IC and suppliers across various supply chains.

- **Forecasting Risks in the Global Supply Chain:** ARLIS researchers are developing a proof-of-concept demonstration applying artificial intelligence (AI) and predictive analytics to forecast supply-chain risk management (SCRM). A prototype is in the works to demonstrate real-world scenarios. The use of ARLIS's CSIFT tool (see "Augmenting Collective Intelligence") can also contribute to this forecasting mission by leveraging "collective intelligence.

[2] "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War." Report by the MITRE Corp. Aug 2018. https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security

- **Supply Chain Proving Ground Using Modular Digital Twins:** ARLIS will develop a modular supply chain digital-twin environment for rapidly testing and validating technology and standards to ensure they meet our nation's security and counterintelligence needs before being deployed. The digital-twin environment supports exercising supply-chain threat vectors for probing, assessing, and mitigating risk by supplying live and virtual simulations.

5G RESILIENCE FOR TODAY'S INTERCONNECTED WORLD

The fifth generation of mobile telecommunications (5G) brings a substantial shift in both the future of wireless technology and the system architecture that enables that vision. The architectural changes include a strong emphasis on software-enabled customization and virtualization of network functions, edge computing, open interface specifications, and the use of commodity hardware. 5G will bring even greater integration of mobile telecommunications with business, critical infrastructure, and defense systems. Therefore, government entities have raised concerns over potential threats that could affect how this technology will be used and implemented.

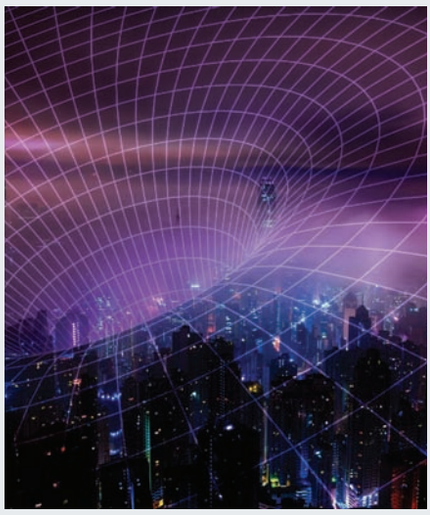
ARLIS is building off A&IS insights and leveraging expertise in wireless communications and cybersecurity to help DoD understand the unique threats and how the U.S. can operate through untrustworthy networks. We are collaborating with both the government and industry to devise a framework to identify gaps where DoD needs to focus investments, including how to work efficiently with commercial industry and prioritizing protections to meet unique DoD operational security needs beyond what is anticipated to be developed commercially. In 2020 ARLIS began building an on-campus test facility for in-depth analysis and experimentation with emerging 5G capabilities and security concerns, including a shielded Faraday Cage enclosure for over-the-air testing and an open-source network-software testbed.

5G/XG SECURITY FRAMEWORK

The 5G/XG Security Framework activity will catalyze a community of key stakeholders across industry and government to refine the framework for security of 5G-to-XG systems and initiate targeted efforts to mitigate prioritized risks.

5G COMMERCIAL HARDWARE TESTBED

In collaboration with researchers on the UMD campus and from U.S.-based telecommunications equipment manufacturers and operators, ARLIS is developing a working knowledge of 5G security features. To that end, the ARLIS testbed includes access to emerging 5G commercial equipment and software, both the radio access network (RAN) and the core network. Testbed experiments will be complemented by formal methods for modeling software-based network control functions. ARLIS is also collaborating with Morgan State University to devise and evaluate novel security features for Internet-of-Things (IoT) devices.



Modeling and Mitigating Insider Risk

One of the most difficult challenges any organization faces is balancing risks: that is, having to accept risks in order to compete against external threats and adversaries — who are seeking to gain an advantage over their competitors using various tools and strategies — while trying to reduce risks of its own assets being compromised by potential "**Insider Threats**." This challenge is particularly important for national security organizations, where their ability to find this balance can literally be the difference between life and death.

Insider Threat programs are only effective to the degree that they both reduce an organization's risks of Insider Threat while also enhancing its performance and its competitive advantage. As the information age gives way to the network age, competitions are increasingly being defined and decided by interconnected human and technical networks. This balance may 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. Accordingly, ARLIS has two immediate key objectives for its MInR efforts:

OBJECTIVE 1: SHIFTING THE PARADIGM

ARLIS is seeking to help the USG move — culturally, technically, and operationally — beyond current "insider threat" models towards an "insider risk" paradigm. Insider threat frames the problem as one of categorization — someone is, or is not, a threat. This binary orientation tends to focus on the person as the source of threat and often ignores the wider context, implying that solutions are mainly about "neutralizing" threats. Further, this may limit those solutions as they often depend upon leveraging the very people who themselves are potentially being categorized as "threats."

In contrast, an insider risk paradigm:

- invites nuance in terms of assigning degrees of risk, and does not fall into categorical thinking;
- is inherently dynamic, since assigning risk necessarily requires taking past behavior, current contexts, and risk forecasts into account;
- focuses on managing — versus eliminating — risk, since risk of any kind will rarely ever go to zero;

- forces one to think about the interaction of individual and contextual variables in quantitative terms, since risk exists at many levels; and
- acknowledges the need to have people be part of the solution in helping to reduce risk of any kind.

OBJECTIVE 2: FLIPPING THE SCRIPT

To reduce risk without compromising performance and organizational competitive advantage, ARLIS is developing the concept of "Insider TRUST," a shorthand for building and maintaining ***Trustworthy, Resilient and Useful Systems and Teams*** (Insider TRUST). Insider TRUST is focused on preventative, rather than reactive, factors and measures that can help identify and address risks and future failure modes, long before concerning behaviors or damaging events occur. Insider TRUST could help inform better risk-mitigation strategies and decisions by understanding and modeling the factors that can enhance trustworthiness and cohesion among individuals, organizations, and systems. Trusted insiders and supportive organizational cultures can increase organizational security and resilience; the challenge is to quantify the degree to which those mitigate different kinds of Insider Risk.

CURRENT VENTURES

Modeling and mitigating Insider Risk is, at its heart, a socio-otechnical problem, with all the attendant challenges of trying to understand, model, and forecast highly variable and complex human social behaviors occurring in, and across, increasingly technologically-enabled and interconnected systems. Accordingly, substantive solutions must be derived from a broad range of disciplines and tools that are required for dealing with complex human systems — from the social and behavioral sciences that help us understand how and why different humans behave in different ways under different conditions, to machine-learning, data science, and AI that can help automate the detection and prediction of patterns in noisy, complex systems.

In 2020 ARLIS MInR efforts include a multifaceted research and development program around Insider Risk and Insider TRUST, government-serving test and evaluation tasks, along with thought leadership and education for the community through a summer training program and a seminar series bringing together government, academic, and commercial industry to promote new perspectives on MInR.

AI and Autonomy for Performance Augmentation

In recent years there has been tremendous progress in the development of **Artificial Intelligence (AI), Autonomy, and Augmentation (AAA)** technologies. While results reported by the research community show great potential, the operational benefits of AAA technologies within the Department of Defense (DoD) and Intelligence Community (IC) have yet to be fully realized. Researchers need to develop processes, methodologies, supporting tools, and testbeds to create AAA-powered applications that reliably perform tasks as intended, perform those tasks in a way that fits naturally within an operator/analyst workflow, produce outcomes that the users trust and understand, and are hardened against malicious attacks. As a trusted agent to the DoD and IC, with core competencies in sociotechnical systems, ARLIS is dedicated to applying a human-centered approach to incorporating into operational workflows AAA technologies that are trusted, reliable, and safe.

In 2020 ARLIS began 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 as well as evaluating the security and robustness of AAA technologies (e.g., via red teaming via adversarial methods). 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, design and evaluate human-machine teams, and conduct user-centric operational test and evaluation. Finally, ARLIS is performing R&D to enable the operationalization of AAA. This includes formal methods and simulation-based verification to support test, evaluation, verification, and validation (TEV&V) for artificial intelligence and autonomy, peripheral nerve stimulation, and blended reality displays for prototyping and demonstrating next-generation cognitive augmentation.

At the request of the Office of the Director of National Intelligence (ODNI) and in partnership with Carnegie Mellon University's Software Engineering Institute, ARLIS is building an R&D roadmap for AI system engineering.[3] Part of this process is facilitating research across academia focused on developing tools and methodologies for a robust process which includes formal methods for AI-based system specification and verification, simulation-based test and evaluation, man-machine teaming and human-computer interaction.

[3] This effort was specifically referenced by the National Security Commission on Artificial Intelligence in its Second Quarter 2020 Recommendations, as work that will benefit the creation of an AI testing framework. (https://www.nscai.gov/reports)

PUTTING HUMAN-SYSTEM INTEGRATION TO THE TEST

ARLIS is currently developing a testbed to evaluate AAA technologies at the mission-level for the intelligence and security communities — to maximize the overall quality of support the tools provide, identify how they might be best employed, and anticipate how they might be harmful. This facility will enable ARLIS to test a wide range of scenarios in purely technical settings and in the context of operational user workflows. As part of this effort, ARLIS is building out a new Human-Computer Interaction Laboratory (HCIL) within its secure facility, which will accommodate usability and accessibility evaluation for a wide range of AAA technologies including information visualization, extended reality, and AI solutions. The HCIL will be used for tasks ranging from incremental usability evaluation early in development to final test and evaluation feedback. By ensuring that the technologies which operators and analysts will use in the future are optimized at the sociotechnical system level, ARLIS testbeds and labs will increase effectiveness for new, emerging AAA technologies as well as improve capabilities across the IC and DoD.

PHYSIOLOGICAL FACTORS OF HUMAN PERFORMANCE

The field of human performance is in a moment of rapid expansion. Technological advancements have made it possible to study, predict, and improve human performance with a precision previously unimagined. Wearable and increasingly sophisticated physiological sensors provide rich and nuanced data about individual traits and states. The availability and quality of physiological data make it possible to examine performance factors outside of the lab and, thus, accelerate the transition from basic to applied research.

Hand in hand with the need to collect large amounts of continuous and high-resolution data is the ability to analyze it. Recent advances in data analytics (e.g., AI and machine learning) have enabled researchers to model and understand physiological data in unprecedented ways, increasing the capability for detecting patterns and profiles to better understand the neural, cognitive, and biological factors that affect performance. Beyond increased understanding, the ability to influence and improve performance is at our fingertips.

ARLIS is a leader in the field of human performance, with its capabilities in:

- Psychometric assessment, including the development of batteries of aptitude tests to improve selection in training and workforce contexts (e.g., cybersecurity and language training;
- Neuroimaging and psychophysiological index development, including improved understanding of how cognitive load and affective states influence performance;
- Physical activity measures, including the relationship between physical activity/ability indices (e.g., accelerometer, gait, cardiovascular health, and lifestyle information) and performance;
- Interventions to enhance performance, including the development and testing of noninvasive peripheral nerve stimulation (PNS) techniques to enhance learning and performance;
- Speech and national language processing, including extracting information about affective and cognitive states based on linguistic output; and
- Team science expertise, both in terms of optimizing trust and usability in human-machine teaming contexts and psychology-based approaches to optimize human team performance.

Of note, ARLIS advances in noninvasive peripheral nerve stimulation techniques have spurred a surge of interest in these approaches to enhancing cognitive and physical performance, including in areas as disparate as reducing cognitive bias in analysts and reducing PTSD effects in service members.

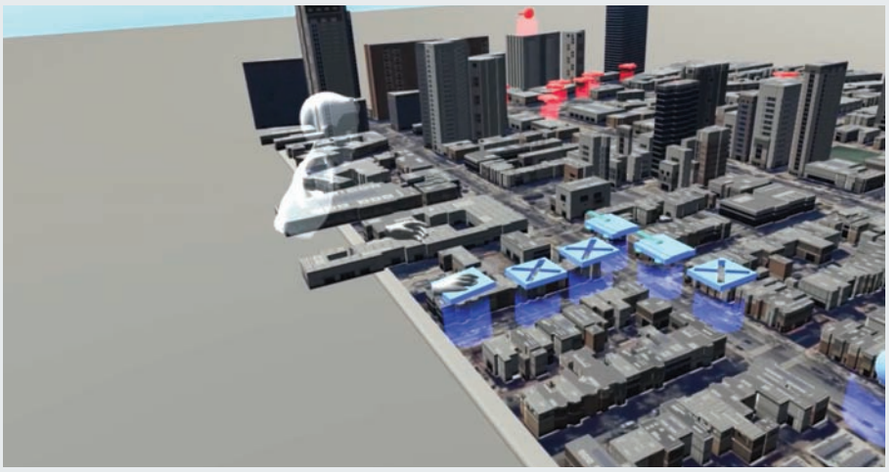
SOME CURRENT VENTURES

A TRUSTED PARTNER TO ENABLE AI INNOVATION

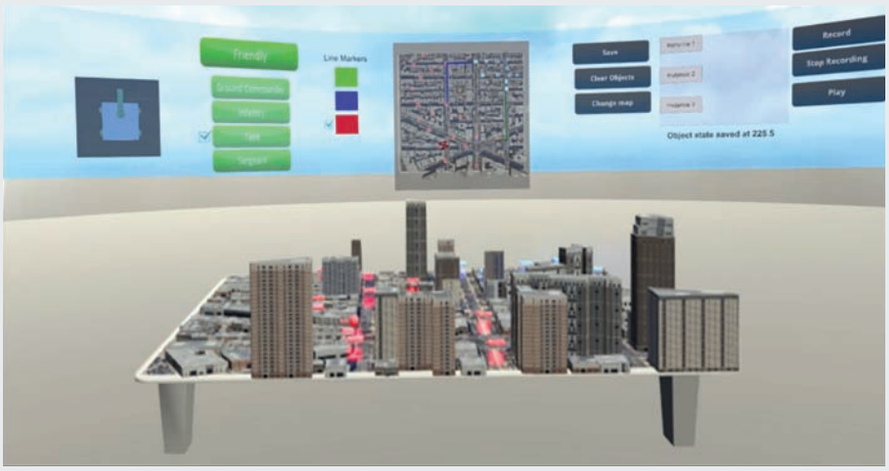
The ARLIS team is a trusted evaluation partner on the DARPA's Hierarchical Identify Verify Exploit (HIVE) and Software-Defined Hardware (SDH) programs. Both of these programs are part of DARPA's Electronics Resurgence Initiative, which in this capacity is developing and running experiments for the AI/ML-accelerator technologies being developed under the programs. These technologies include cutting-edge, experimental hardware designed to support hybrid sparse-dense machine learning workflows and large-scale graph analytics, as well as algorithms to support a variety of mission-critical tasks. ARLIS is playing a key role in every step of the testing and evaluation life cycle, from problem identification and dataset selection/generation to performance analysis, including scalable, reproducible benchmarking for the purpose of trade-off aware comparative analysis.

AI AND VR TO AUGMENT MISSION PLANNING

In 2019 and 2020, ARLIS worked with a team from the Army Futures Command C5ISR Center to develop a prototype distributed collaboration tool based on virtual reality (VR) technology. The prototype enables physically distributed commanders to plan and rehearse a mission around a virtual "sand table" as if they were physically co-located. The distributed planners collaborate around a virtual representation of the physical terrain, building plans using standard military symbology, and then rehearsing the scenarios through simulation over constrained communication channels.



Avatar Embodiment:
Team members become virtually collocated avatars and interact with each other and shared objects such as the military symbologies



Roomscape with Tabletop:
Teammates instantiate around a table that shows targeted landscapes, and has a menu to create objects, see a 2D map, save current states, and more

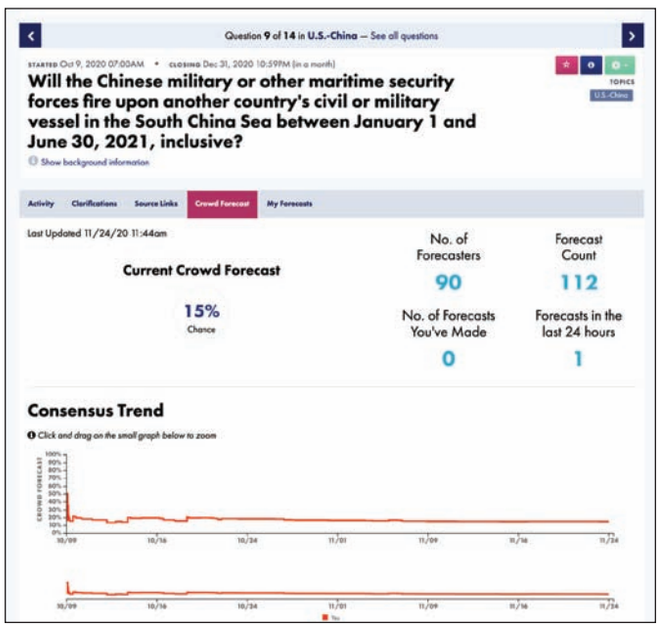
Augmenting Collective Intelligence

Collective intelligence is the "shared or group intelligence that emerges from the collaboration, collective efforts, and competition of many agents and individuals"[4] which enables an organization or group to leverage human diversity, strengths, and capabilities to make better decisions than could be made by any single individual or agent. While cooperation is commonplace among humans, collective intelligence can also be fostered through technology that structures more effective, larger-scale collaboration and aggregates the results to create high-quality outputs. Collective intelligence tools are of value in making decisions where:

- There is a lack of clean, historical data to build comprehensive models;
- The future may have little to no resemblance to the past;
- Numerous variables and outcomes must be taken into account along with complex, hard-to-measure causal factors;
- There are regular streams of new information that must be weighed and considered; or
- There is a possibility of surprise events that likely wouldn't be found in existing data patterns.

Making predictions about the future is one area where enhanced collective intelligence could dramatically improve the state of the art. Accurate forecasts could provide significant decision advantage, but — despite significant technological advances for predicting certain types of outcomes — they still depend heavily on human judgment. While most decision-makers are under constant pressure to make critical decisions, the evidence suggests that most people are poor at making individually accurate forecasts. However, collective intelligence — in the form of aggregating many individual forecasts using networks and platforms — has demonstrated success in enhancing the accuracy of forecasting. Accordingly, ARLIS is leveraging technology and a decade of lessons learned from the Intelligence Community Prediction Market to launch the Crowd Security and Intelligence Forecasting Tool (CSIFT) to "augment" collective intelligence by eliciting and collecting probabilistic forecasts from cleared experts across agencies; aggregating forecasts to show changing consensus over years, months, or days in advance; and providing analyses and results for integration into reports and products for decision advantage.

Along with CSIFT, our current and future goals in augmenting collective intelligence are two-fold: foundationally, we seek to provide direct support to intelligence and security missions through the operationalization of collective intelligence technologies, including forecasting, decision science, and cognitive augmentation. At the same time, we seek to continuously augment collective intelligence through innovative and quantitative R&D, advancing the science of how to best enhance and aggregate human intelligences, as well as developing and demonstrating methods to combine machine intelligences with humans' for further decision advantage.



[4] Collective intelligence, https://en.wikipedia.org/wiki/Collective_intelligence (last visited Dec. 7, 2020).

Language and Culture as Research Enablers

ARLIS's origins as a UARC were focused on comprehensive language preparedness for the 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, and derived from social media. Beyond our work in human language technologies, our linguists and language experts are directly involved in many of ARLIS's current projects, along with the direct generation of high-quality data resources for government and research communities.

Communication is a crucial way to interpret disinformation campaigns and understand how the global population interacts with computer systems. For example, a cross-disciplinary team of ARLIS researchers combined their expertise in Russian language, psychology and cognitive sciences, and computational linguistics on a ground-breaking project classifying an author's personality traits in Russian social media content. Additional social media projects are gaining new insights into how emotions influence the resharing of content on Eastern European social media, tracking Chinese influence in Kenya as part of its Belt and Road Initiative, and investigating the spread of disinformation related to the COVID-19 pandemic.

DATASET PROVISIONING

ARLIS maintains a curation of high-quality, purpose-built language datasets. Specializing in under-resourced world languages, our scientists can craft research projects that involve any human language on earth. We combine traditional and cutting-edge language data collection methods and utilize automated processes to facilitate, rather than replace expert human curation. Over its history, ARLIS (and CASL before it) has curated, normalized, and annotated linguistic data in a multitude of languages for our government clients for a broad range of analytic purposes. This research includes the fundamental resource development for unfamiliar languages as well as the analysis of rhetorical constructions, annotation, and multilingual social media data. These datasets have facilitated and upgraded the development of speech-to-text, text-to-speech, automatic speech recognition, machine translation, translation memory, cross-language information retrieval, reference-tracking, emotion detection, sentiment analysis, personality classification, authorship attribution, and a range of other data analytics, as well as language identification and high-level language learning.

- Arabic
- Bambara
- Bangla (Bengali)
- Chimwiini
- Chinese
- Dhivehi
- Hausa
- Korean
- Pashto
- Persian
- Polish
- Portuguese
- Punjabi
- Russian
- Somali
- Swahili
- Tamasheq
- Ukrainian
- Urdu

ARLIS researchers have generated data resources in the languages shown for both operational and academic use.

Programs and Partnerships

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 UMD 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's proximity to the nation's capital has resulted in many research partnerships with the federal government. This allows students and IC professionals to work alongside ARLIS researchers to create new academies and foster internship programs.

ARLIS is devoted to the University of Maryland's pursuit of academic excellence, prospering the success of the State of Maryland, and providing immediate service and effective solutions to the needs of the United States Department of Defense and Intelligence Communities.

Training Programs

CONNECTING TECHNOLOGY, SECURITY, AND LAW

Recognizing the need to arm IC attorneys and policy practitioners with skill sets to excel in a national security landscape, ARLIS held a six-week program in June of 2020 that trained 31 legal and policy professionals from the defense and intelligence communities on various aspects of information technology and how the growth of IT is changing the dynamics of law.

Emerging Topics in Technology and Law is the first of a set of accredited courses held through UMD's School of Public Policy, leading to a planned certificate and master's level degree program in Technology, Law, and National Security. More than 20 instructors with diverse areas of expertise gave lectures ranging from cybersecurity to international law to misinformation.

The students represented almost all the U.S. government agencies across the DoD, the armed services, and the Intelligence Community. Considered to be the best and brightest by their senior leaders, the pupils gained in-depth knowledge of the IT technologies relevant to current and future DoD/IC missions. However, the course's salient theme addressed how humans interacting with technology can create formidable legal and policy challenges. ARLIS plans to offer more courses in 2021, in a classified setting and with more than a hundred participants, to help produce the next generation of cyber legal professionals to aid the intelligence and security community.

MENTORING FUTURE LEADERS IN SECURITY RESEARCH

The **AI Research for IC Challenges (AIRICC) Internship Program,** piloted in 2020, prepares and nurtures a pipeline of student talent, at the graduate and undergraduate level, to be the next generation of AI leaders. AIRICC aims to both expose talented computer scientists to meaningful immediate security problems and to build personal connections to government technologists who are currently attempting to solve these problems. The inaugural 10-week program, which ran June through August, was sponsored by the National Geospatial-Intelligence Agency. The NGA funded the program to challenge students with current mission-driven applications that the NGA uses to solve real-world scenarios, which included exploratory research inspired by the neocortex in the brain, hurricane track prediction, the identification of traffic anomalies using sparse data, distinguishing sea vessels and icebergs using low-resolution satellite imagery, and the analysis of AI applications used in engineering systems.

Eighteen competitively selected interns (fifteen undergraduates and three graduate students) came together to work in teams of three. While most hailed from UMD, one intern came from neighboring Bowie State University, reflecting ARLIS and the IC's interest in bringing more talent from Historically Black Colleges and Universities (HBCUs) into the national security technologist pipeline. Their disciplines included computer science, biology, mechanical engineering, computer engineering, and aerospace engineering. The second iteration of the AIRICC program will be conducted in the summer of 2021.

Modeling and Mitigating Insider Risk: ARLIS, in coordination with START and faculty from the University of Maryland, is organizing a 10-week course in Summer 2021 comprising a "comprehensive and tailorable professionalization program" that equips the future workforce with the skills to model and mitigate insider risks within DoD and other national security-relevant organizations and industries.

The program has an education and training component (including UMD prerequisites). involves a portfolio of 10-week projects at an advanced undergraduate or graduate level, and will create a cohort of 10–15 student scholars working with faculty and U.S. government advisers on Insider Risk education. The course will also bring together students and operators through creative and experiential methods — including the use of "risk-gaming" and deep dives into risk assessment tools — as well as trips to DoD and IC facilities as available (i.e., CIA Museum, NSA Crypto Museum, NIU, etc.). Ultimately, the program will expose students to the diversity of challenges and opportunities for modeling and mitigating Insider Risk for national security.

Partnerships in Higher Education

THE INSURE CONSORTIUM: SECURING AND PROTECTING NATIONAL SECURITY INTERESTS

In 2020 ARLIS stood up the Intelligence and Security University Research Enterprise (INSURE), an academic research consortium to further its mission as a UARC supporting the Defense Security Enterprise (DSE) and the IC. Consortium partners are selected based on symbiotic institutional strengths, having a track record of conducting applied, quick-turn, mission-relevant R&D, and offering unique capabilities for training the current workforce and growing the workforce of the future. INSURE has initially brought in a targeted set of six initial partner institutions: George Mason University, Howard University, Morgan State, Texas A&M University, University of the District of Columbia, and the University of Wisconsin in Madison. These schools were brought in to expand the pool of talent and technical resources available for supporting ARLIS core competencies and to increase the agility with which higher education resources can be harnessed for national security needs.

Modeled in part on the consortium approach of the Systems Engineering Research Center UARC at Stevens Institute of Technology, ARLIS and its university partners coordinate applied and use-inspired research activities for Intelligence and Security at associate Universities, aligning projects with specific DoD and IC program managers and activities. This alliance improves the translation of products into operational use and enhances the pipeline of students and faculty to work directly on technology problems for the national security community.

Spring and summer 2020 activities have included candidate member engagement (coordinating in part with the Office of the Secretary of Defense team overseeing DoD investments in HBCUs); developing consortium agreements and master subcontract agreements to administratively streamline management; proposal development and submission yielding three consortium awards in September 2020; and working to build a financial model for resourcing consortia leadership activities from 2022 onward. In the year ahead, activities will include:

- Joint program development for the member universities with the DoD/IC;
- Developing curricula for courses, training, and certificates for employees of the DoD/IC;
- Organizing an INSURE Security Research Day for legislators on Capitol Hill and a 2-day INSURE Workshop for the DoD/IC to be held at ARLIS in 2021
- Building an inventory of shared testbeds, facilities, capability descriptions accessible to the DoD/IC via the consortium (i.e., AI V&V/T&E, computing, data curation, etc);
- Establishing a shared plan for management of Controlled Unclassified Information (CUI) or restricted datasets, virtualization of desktops for R&D by the consortium; and
- Coordination of student activities across all relevant disciplines.

ARLIS External Advisors

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.

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.

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.

Dr. Jason Matheny is founding director of Georgetown's Center for Security and Emerging Technology (CSET), and previously served as Assistant Director of National Intelligence and Director of IARPA.

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

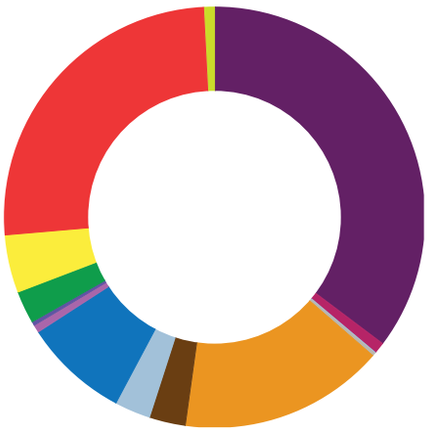
Since its inception in 2018, ARLIS has experienced exponential growth. During the fiscal year that ended September 30, 2020, ARLIS earned revenue from awards and contracts totaling $54 million compared with $15 million for the previous fiscal year (and $2 million in FY18). As a non-profit University Affiliated Research Center, the revenue we earn is invested in our research and development endeavors, our facilities, and educational programs.

The figures below illustrate the distribution of the $54 million in new awards made in FY 2020, 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 FY20

- A&IS
- AAA
- Aptitude
- COGSEC
- Computational Infrastructure
- Language & Culture
- MInR
- Programs
- SME
- Other Research

Sponsorship Profile
USG FY20



- Army
- DARPA
- IARPA
- Industry
- NGA
- NSA
- ONR
- Air Force
- OSD Strategic Capabilities Office
- SOCOM
- USD for Acquisition & Sustainment
- USD for Research & Engineering
- USD for Intelligence & Security

Project Types
USG FY20

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

SME = Subject Matter Expertise
MInR = Modeling and Managing Insider Risk
A&IS = Acquisition & Industrial Sec
AAA = AI, Autonomy, & Augmentation
ARLIS Programs = training programs like those described in the report

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