APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

RESEARCH FOR INTELLIGENCE AND SECURITY CHALLENGES

>> 2023 INTERNSHIP PROGRAM

PROGRAM REPORT / FALL 2023

RESEARCH FOR INTELLIGENCE AND SECURITY CHALLENGES

INTERNSHIP PROGRAM

RISC Program Report

RISC: CREATING AND NURTURING STUDENT TALENT

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

The RISC internship program creates and nurtures a pipeline of student talent at both graduate and undergraduate levels, providing outstanding students an opportunity to work on real-world problems within ARLIS focus areas as a university-affiliated research center and, in the process, to learn about sponsor missions and career opportunities in the defense intelligence and security enterprise.

Leveraging Talent Nationally to Address Real-World Challenges

Since there is no one-size-fits-all solution to real-world intelligence and security challenges, ARLIS draws from a wide pool of disciplines and higher-education institutions for the RISC program.

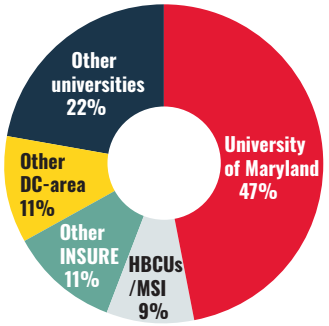
RISC targets students from various disciplines including science, technology, engineering, mathematics, and social science fields. Many of the students come from the University of Maryland, but the majority come from other institutions, including the ARLIS-led Intelligence & Security University Research Enterprise (INSURE) consortium and Historically Black Colleges and Universities (HBCU). This broad reach is made possible in part by the predominantly virtual framework for collaborative work.

Each year, evaluators consider a talented applicant pool to identify RISC interns. They are measured by demonstrated strengths in relevant fields, experience working both independently and in teams, and demonstrated interest in contributing to national security. All U.S. citizens enrolled in an accredited university program—particularly rising juniors, seniors and early graduate students—are eligible and encouraged to apply.

PROGRAM GOALS

- Attract and train the future cleared technical workforce of the Intelligence Community and the Defense Security Enterprise.
- Real projects for real end-users: Work on stuff that matters!
- Help students learn about national security careers and engage directly with members of security and intel communities.
- Expose students to research: i.e., self-directed exploration and experimentation with open-ended questions, conducted with rigor.
- Attract new faculty researchers to applied work in the national interest.

WHERE OUR 2023 RISCers COME FROM



"The chance to engage with real government challenges at a young age and early career phase is a unique and invaluable opportunity that RISC offers. This program not only enhances one's skills and understanding of modern-day national security issues, but also serves as a motivating and driving force going into the academic year."

–RISC INTERN TESTIMONIAL

"The networking I have done and the connections I have built have made me hopeful for my future career and applying to government and intelligence jobs."

–RISC INTERN TESTIMONIAL

2023 INTERN DEMOGRAPHICS

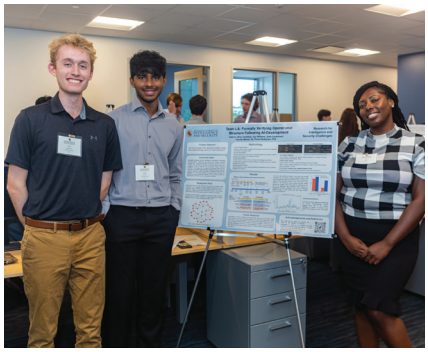
- **122 interns** from 42 institutions selected **from 383 candidates**
- 83 undergraduates or recent grads
- 25 MA/MS students
- 14 PhD/JD students
- **14** returning interns from RISC 2022
- **11** interns from HBCU / MSI schools
- 78 interns from INSURE Consortium universities (58 from UMD)
- 47 interns from outside the National Capital Region

Disciplines of Interest

Specifically, the RISC initiative sought outstanding undergraduate and graduate students with expertise in the disciplines listed below.

1. **Computer Science, Information Science & Engineering:** AI/ML algorithmic development, HCI, software engineering, systems engineering, media analysis and forensics, information systems design, geographic information systems, AI assurance, human-system integration;
2. **Mathematics and Statistics:** Data analytics, quantitative modeling, experimental design, graph analytics;
3. **Social & Behavioral Sciences:** Cognitive/neuroscience & psychology, sociology, criminal justice, teamwork and group dynamics, communications, disinformation and misinformation, social network analysis, anthropology, human geography (e.g., pattern of life/ mobility modeling), political science, international relations;
4. **Languages and Linguistics:** Languages of interest to global security including but not limited to Mandarin, Russian, Farsi, Korean, and Arabic; computational linguistics and natural language processing; natural language understanding;
5. **Data Science:** Data and knowledge engineering, data curation, tagging, metadata, repositories, data visualization, library sciences;
6. Additional topics including: Measurement and evaluation of learning outcomes, environmental modeling and remote sensing, human factors, and regulatory public policy.

In 2023, ARLIS received 383 applications from 81 universities and 122 students were selected from 42 universities. The students selected for RISC 2023 brought backgrounds including:



John Lauterbach (UMD), Varun Unnithan (UMD), and Joy Williams (Morgan State) supported an ODNI project on "Formally Verifying Operational Structure Following AI-Deployment" (LA).

RISC interns enjoy their first opportunity for face to face engagement at the Intern Lunch.

TEAM ID: Rachel Rodriguez Spradley (University of South Carolina), Trinity Gipson (Texas A&M), and Rachel Stoneking (Georgetown) brief their project to a government representative.

The class of 2023 supported 48 projects benefiting 23 defense and intelligence agencies. Project topics included:

- Developing unified methodology for diagnosing infrastructure cyber risk, including a scoring metric for quantifying cyber risk, and a software tool that automatically calculates this metric for bases and their infrastructure sectors.
- Deriving a standardized and repeatable procedural framework that employs natural language processing (NLP) capabilities into an algorithmic pipeline for consolidating potentially overlapping Security Declassification Guides.
- Examining responsible ways to incorporate open-source AI into missions.
- Conducting test and evaluation for a service to improve interactions with international audiences.

All project titles and project abstracts from 10 of these 48 projects are included in this report, representative of the wide range of problems tackled.

The RISC Experience

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

The program is structured to facilitate interactions within teams, between teams, and with government sponsor representatives. Interns attended weekly seminars and regular team development meetings in a shared virtual work environment, although select projects may require on-site work. The summer program concluded with several days of in-person activities in College Park, Md., where attendees discussed project outcomes with peers and visiting experts from the defense and intelligence

"RISC 2023 allowed me to advance my interest in working in the Defense and Intelligence Sector by initiating my clearance investigation and providing me connections with individuals who used to or currently work in these areas, thereby informing me of what their career was like."

–RISC INTERN TESTIMONIAL

"This program helped to solidify my interest in going into the defense/intelligence world. It provided me with a window into how governmental research works and how, as civilians, we can help further the mission of the IC." –RISC INTERN TESTIMONIAL

At the 2023 RISC Research Showcase, faculty mentor Eric McGlinchey (George Mason) asks Philip Ly (University of North Georgia) and Ignacio Valdez (UMD) about the analytical planning tool they built for the Army.

Team MT: Caroline Gish (Georgetown University), Tejasri Pavuluri (UMD), and Fei Yang (UMD Global Campus) work to prepare their remarks for the Research Showcase ahead.

"While I was already committed to a career in national security, the RISC program further solidified my dedication to the mission of the IC. As a Cybersecurity Engineering student with a minor in Intelligence Studies, I had a somewhat narrow view of potential cyber career paths. However, through networking, I became familiar with a wide range of opportunities across the government, as well as new job interests including roles like cyber supply chain security, which extend beyond purely technical positions."

—RISC INTERN TESTIMONIAL

communities and gained greater context on how the work fits into government sponsors' mission space.

Given mutual interest between the sponsor and interns and available funding, RISC projects often continued into the academic year, sustaining sponsor connectivity beyond the original 10-week period. In 2022, 37 interns continued their work at ARLIS; at the time this report went to print, approximately 50 interns were expected to continue work with ARLIS into the fall.

Connecting Interns to the Intelligence and Security Communities

For additional exposure to intelligence and security issues, the RISC interns also participate in a series of midday lunch-and-learn sessions led by ARLIS faculty and staff who brief about varying topics including, overviews on the intelligence community and the Defense Department; countering malign influence; quantum and tech defense careers; using the presidential daily briefing as an example of how to present effectively; security and diplomacy; ethical, legal and social implications; cyber operations; and special operations.

Extending the lunch-and-learn model, 2023 RISC program staff facilitated a number of small group discussions between four-to-eight interns and a current or former senior official from the defense or intelligence communities. Supplementing the large-group lunch-and-learns, the small group sessions enabled multiparty discussion on topics like careers in counterintelligence, government-wide stakeholders working to countering malign influence, and how military cyber security work differs from elsewhere.

In addition, RISC organized a number of sessions for interns to learn about pathways to careers in the intelligence and security communities. This included a broad discussion on how to plan and what to expect in the application process, DoD Scholarship-for-Service opportunities for those in STEM fields, and a plenary discussion from the senior executive for human capitol for the defense intelligence and security communities at the final week events.

Technical Guidance from Top Faculty

A critical component of the RISC intern research experience is working with a team of peers under the technical guidance and mentorship of university faculty members with expertise in relevant fields. Faculty mentors play a second critical role working with the government sponsor to help translate a given proposed security problem into a scoped project that can be tackled over the short 10-week program.

In 2023, 49 mentors supported the 48 projects, with only 16 from ARLIS directly and the remainder recruited from across the University of Maryland and other institutions in the ARLIS-led INSURE consortium including HBCUs Howard University and Morgan State. 25 mentors returned from RISC 2022, providing their previous talents and insights for ARLIS to engage for future intelligence.

Beyond ARLIS, the 2023 University of Maryland faculty mentors came from UMD's School of Public Policy, the Departments of Aerospace Engineering, Computer Science, Civil & Environmental Engineering and the Center for the Study of Terrorism and Reactions to Terrorism.

"One of my goals was to explore topics outside my expertise. I'm very pleased with the outcomes of the projects I mentored and look forward to continuing to further my interests in my chosen projects."

—DR. CLISTON COLE, ASSISTANT PROFESSOR, MORGAN STATE UNIVERSITY

"I have worked with hundreds of sharp students as well as partnered with many USG colleagues. The Team AL cohort was among the best I have worked with in my academic career."

—ERIC MCGLINCHEY, PROFESSOR, GEORGE MASON UNIVERSITY

Team TX interns Lina Gomez (UMD) and Laurie Jones (University of Colorado Boulder) talk with faculty mentor Pete Loats (UMD ARLIS).

Faculty mentor Onyema Osuagwu (Morgan State University) talks to interns Sveta Bartholomew (University of Wisconsin), Nour Ali Ahmed (UMD), and Niels Brandon (UMD).

"Being part of the IC community where your ideas are taken into consideration and you are paired with informed people to tackle national problems is a great reason to participate in next year's RISC program."

–RISC INTERN TESTIMONIAL

"The project topic was intellectually stimulating and relevant to both my current portfolio and engagement with the government sponsor."

–RISC FACULTY MENTOR TESTIMONIAL

RISC 2023 interns, mentors and program team.

"This program allows you to be exposed to topics and people outside of your typical area of study/outside of your comfort zone, which is a great learning and growth opportunity."

–RISC INTERN TESTIMONIAL

"If you have the passion to serve and defend your country, this internship is definitely a gateway to doing so."

–RISC INTERN TESTIMONIAL

Highly Engaged Government Champions

The RISC program would not have nearly the impact or learning value without government-provided topics, resourcing, and team engagement to ensure that the work stays grounded in applied missions. In 2023, ARLIS had the privilege to work with USG topic champions representing 23 distinct organizations within the defense intelligence and security enterprise:

- **Undersecretary of Defense for Intelligence and Security—core sponsor**
  - Physical and Operations Security
  - Influence & Perception Management
- **National Geospatial-Intelligence Agency—core sponsor**
- **Office of the Director of National Intelligence—core sponsor**
- Army
  - G-2 Fusion OIC, Personnel Security
  - III Armored Corps G2/SIO
  - Army Research Lab
  - Army Futures Command
  - Corps of Engineers
  - 1st Special Warfare Training Group
  - Army Special Operations Command (USASOC) Deputy G6
- OSD Minerva Research Initiative
- Naval Air Warfare Center
- OSD Chief Data and Artificial Intelligence Office (CDAO)
- Defense Counterintelligence & Security Agency (DCSA)
  - Industrial Security
  - National Center for Credibility Assessment
  - Security Training Directorate
- OUSD(Acquisition & Sustainment) CISO/Cyber Warfare
- OUSD(Research & Engineering)
  - Maintaining Tech Advantage
  - S&T Program Protection
  - HBCU/MSI office
- Washington Headquarter Service Records & Declassification Division
- ARLIS projects from DARPA, ONR, DCSA, IARPA, elsewhere

"Every single speaker or mentor took the time to learn about us and ask questions, give advice, and share their experiences."

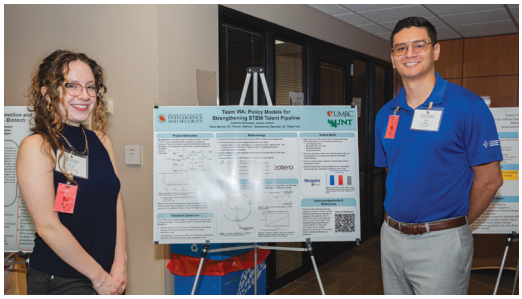
—RISC INTERN TESTIMONIAL

RISC Project to ARLIS Program: Declassification Modernization

Government agencies responsible for declassifying mounds of documents are about to be hit with even more in 2024, when a requirement to digitize all records goes into effect and generates 500 million more pages of records requiring attention. New modern, non-manual processes will be needed to meet these federal mandates.

While modernizing DoD declassification has become a major ARLIS research activity (funded at $6.5 M to date), its efforts started with a small RISC internship project in Summer 2021. That team performed detailed policy analysis and interviewed subject matter experts to identify inefficiencies and gaps and draft a framework for modernizing DoD declassification. Building off that work, in 2021 and 2022, ARLIS evaluated and assessed new technologies and approaches to manage the document classification and declassification processes, and tested capabilities best suited for the declassification workflow. RISC 2022 then saw two new intern projects—funded by the Air Force and OUSD(I&S), respectively—to investigate technologies for consolidating security classification guides and to understand meta-data standards for improving accession to NARA. And in 2023 RISCers considered how to consolidate and align the 1700+ declassification and security classification guidelines across agencies, informing an overall process that ARLIS is developing to use artificial intelligence to ease the declassification burden on agencies.

This growth demonstrates the value of RISC not only for the I&S workforce, but as a sandbox to explore new problems and solutions for the I&S enterprise.



Gabriela Schweers (Harford CC) and James Jenkins (University of North Texas) used systems dynamics modeling for "Policy Models for Strengthening STEM Pipelines" (WA).

Madison Krstich (University of Pittsburgh) and Alex Nulman (UMD) of Team AR answer questions from UMD ARLIS researcher Matt Venhaus.

Sonrisa Reed (University of North Georgia) presents Team NV research on Data Augmentation of Overhead Satellite Imagery to Support Computer Vision.

Program Outcomes

Beyond the training experience and mission exposure, team deliverables vary greatly by project. Some generate a sharable code base, while others generate and brief policy recommendations, often to senior stakeholders. All projects also generate mid-program and final reports and participate in a final RISC Research Showcase event.

ARLIS also helps RISC interns obtain clearances, adding value to the interns' summer efforts and setting students up for national security work in the future.

Ultimately, the RISC program aims to attract new talent to the Defense Department, intelligence community, and larger security and intelligence enterprise by exposing top students to interesting work in support of a compelling mission. Though the program remains young, early data indicate a clear return on investment: of the interns who participated in summer 2021 and had graduated, 81% were employed by the government, the defense industry or ARLIS as of spring 2023. (See "Metrics of Success")

"It's a unique experience where every person is of very high caliber. Every person I spoke to or had the opportunity to listen to took pride that their work was contributing to something greater than themselves or a business."

—RISC INTERN TESTIMONIAL

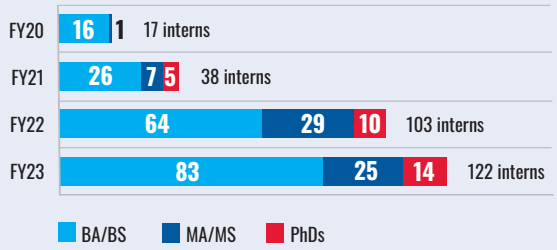
"The RISC program opened my eyes to the world of national security; a field I would never have expected to be pursuing a career in now. The ambiguity of the program allows interns to make the project their own, to interact with government sponsors and develop invaluable relationships with their mentors. The RISC program has given me everything I need to feel confident today as I explore career paths in the IC."

—RISC INTERN TESTIMONIAL

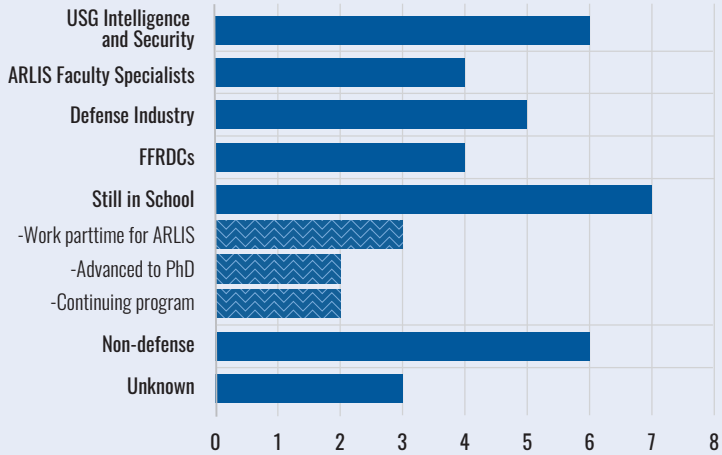
Metrics of Success

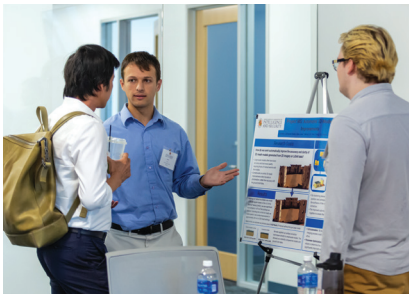
RISC has grown exponentially since its inception, from 17 students the first year to 122 in 2023. Nearly 50 interns will continue working on projects into the fall, and a large majority of the interns have expressed a desire to pursue careers in intelligence and security. As of September 2023, 105 interns from RISC 2023 have been successfully adjudicated for security clearances, which will further facilitate those career paths while also augmenting the credentialed talent pool for the intelligence and security communities. Wrapping up our fourth summer, we are developing richer metrics of how RISC affects student career outcomes.

PROGRAM GROWTH BY NUMBER OF INTERNS

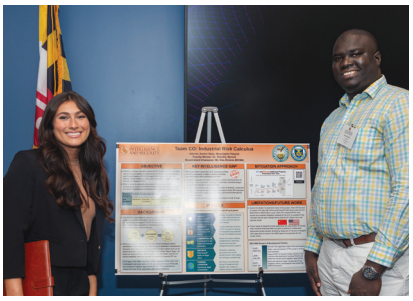


RISC 2021: WHERE ARE THEY NOW

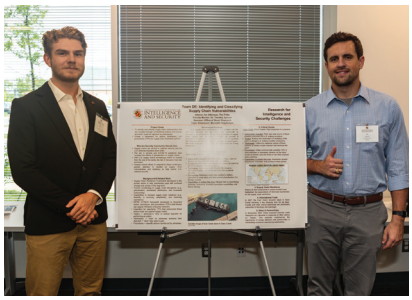




Alan Luner (Johns Hopkins) and Zachariah Davis (Purdue University) describe Team MS work on "Automated 3D Modeling Improvements."



Amber Alam (Texas A&M) and Moustapha Hoyeck (Howard University) applied their backgrounds to support "Industrial Risk Calculus" (CO).



Tim Fritts (University of South Carolina) and Ian Atkinson (Texas A&M) supported research on "Identifying and Classifying Supply Chain Vulnerabilities" (DE).

"I have learned more than I ever expected and am now pursuing a career in national government and defense that I never would have done before this internship."

–RISC INTERN TESTIMONIAL

TEAM AK: ***Technology Promotion and Protection Framework—Biotech***
Champion: Maintaining Tech Advantage, OUSD(Research & Engineering)
Faculty Mentor: **Onyema Osuagwu**, Morgan State University
Interns: **Sarah Bartley** (NC Agricultural & Technical State Univ), **Niels Brandon** (UMD)

TEAM AL: ***Risk Framework for Identifying and Protecting Critical Technology RDT&E***
Champion: Influence & Perception Management, C&SP, OUSD(I&S)
Faculty Mentor: **Eric McGlinchey**, George Mason University
Interns: **Gianfranco Secondi** (UMD), **Lily Bistline** (Loyola Univ Maryland), **William Foster** (Georgetown)

TEAM AR: ***Technology Protection Strategic Risk Framework***
Champion: S&T Program Protection, OUSD(Research & Engineering)
Faculty Mentor: **Marcus Boyd** and **Robert Lamb**, UMD START
Interns: **Madison Krstich** (U Pittsburgh), **Alex Nulman** (UMD), **David Zhao** (Stony Brook University)

TEAM AZ: ***Technology Protection Map Visualization and Synchronization***
Champion: S&T Program Protection, OUSD(Research & Engineering)
Faculty Mentor: **Michelle Bensi**, UMD Civil and Environmental Engineering
Interns: **Ryan Essem** (UMD), **Jin Tae Kim** (Binghamton U), **Lailah Mozaffar** (Georgetown University)

TEAM CA: ***Characteristics of Disruptive Technology for Public Health Applications***
Champion: OUSD(I&S) and U.S. Department of Health and Human Services
Faculty Mentor: **Monique Beaudoin**, UMD ARLIS
Interns: **Wren Lowe** (UMD), **Ellie Tyler** (Virginia Tech)

TEAM CO: ***Industrial Risk Calculus***
Champion: Industrial Security, DCSA
Faculty Mentor: **Tim Sprock**, UMD ARLIS
Interns: **Amber Alam** (Texas A&M University), **Mouhamadou Hoyeck** (Howard University)

TEAM CT: ***Cybersecurity Vulnerabilities in Critical Infrastructure***
Champion: CISO/Cyber Warfare
Faculty Mentor: **Charles Harry**, UMD Public Policy
Interns: **Andrew Lee** (Stanford University), **Olivia Unzueta** (Penn State Dickinson Law)

TEAM DC: ***Futurecasting PRC Belt and Road Initiative Activities Using Contract Language***
Champion: OUSD(I&S) and U.S. Department of Health and Human Services
Faculty Mentor: **Steve Sin**, UMD START
Interns: **William Horton** (UMD), **Ryan Knapick** (Georgetown University), **Will Lennon** (UMD)

TEAM DE: ***Identifying and Classifying Supply Chain Vulnerabilities***
ARLIS Contract Sponsor: Office of Naval Research
Faculty Mentor: **Tim Sprock**, UMD ARLIS
Interns: **Ian Atkinson** (Texas A&M University), **Timothy Fritts** (University of South Carolina)

TEAM FL: ***Tactical information classification policy and procedures***
Champion: US Army Special Operations Cmd, Deputy G6
Faculty Mentor: **Wendi Kaspar**, Texas A&M University
Interns: **Adams Awasum** (UMD), **Morgan Evans** (Penn State)

TEAM GA: ***Technology Insertion for Security Classification Guide Consolidation***
Champion: Records and Declassification Division, Washington Headquarters Service
Faculty Mentor: **Mike Brundage**, UMD ARLIS
Interns: **Thomas Lu** (UMD), **Nitish Vobilisetti** (UMD)

TEAM HI: ***Unauthorized Installation Access***
Champion: Physical and Operations Security Directorate, OUSD(I&S)
Faculty Mentor: **Natalie Scala**, Towson University
Interns: **Noah Hibbler** (UMD), **Joel Stern** (Brandeis University)

TEAM ID: ***Impacts of Continuous Vetting on Resourcing and Risk Management***
Champion: Army G-2 | Personnel Security
Faculty Mentor: **Allison Reilly**, UMD Civil and Environmental Engineering
Interns: **Trinity Gipson** (Texas A&M), **Rachel Rodriguez Spradley** (University of South Carolina), **Rachel Stoneking** (Georgetown University)

TEAM IL: ***Modernizing Credibility Assessment***
Champion: National Center for Credibility Assessment, DCSA
Faculty Mentor: **Daniel Barbara**, George Mason University
Interns: **Cecilia Taylor** (University of South Carolina)

TEAM IN: ***HORIZON project***
ARLIS Contract Sponsor: Defense Counterintelligence and Security Agency
Faculty Mentor: **Harvey Rishikof**, UMD ARLIS
Interns: **Ananya Amirthalingam** (Georgetown University), **James Maher** (UMD)

TEAM KS: ***Processing Operational Data as Business Analytics***
Champion: DoD Chief Digital and AI Office
Faculty Mentor: **Matt Sinclair**, University of Wisconsin
Interns: **Zaid Osta** (George Mason University), **Parthav Poudel** (UMD), Sanjana Sankar (UMD)

TEAM KY: ***Non-Expert Auditing of Open-Source Libraries for Mission-Critical AI Capabilities***
Champion: ODNI and Joshua Poore, UMD ARLIS
Faculty Mentor: **Alan McMillan**, University of Wisconsin
Interns: **Chamarr Auber** (UMD), **Edmund Kargbo** (UMD), **Pradyumna Kotla** (UMD)

TEAM LA: ***Formally Verifying Operational Structure Following AI-Deployment***
Champion: ODNI and Joshua Poore, UMD ARLIS
Faculty Mentor: **Paulo Shakarian**, Arizona State
Interns: **John Lauterbach** (UMD), **Varun Unnithan** (UMD), **Joy Williams** (Morgan State University)

TEAM MA: ***Development of User-Centric T&E Plans to Evaluate an AI Technology that Processes Collected Exploitable Material***
Champion: Brian Weiss, UMD ARLIS
Faculty Mentor: **John Diem**, Texas A&M U
Interns: **Paul Mercer** (Univ of Tennessee), **Tyler Houser** (George Mason), **Rachel Wang** (George Mason)

TEAM MD: ***Simulation-Based Verification for Autonomous Systems***
ARLIS Contract Sponsor: Army Research Laboratory
Faculty Mentor: **Steven Howell**, UMD ARLIS
Interns: **Tomer Atzili** (UMD), **Scottie Tran** (UMD)

TEAM MI: ***Neural Networks for Improved Turbulence Models***
Champion: Naval Air Warfare Center—Aircraft Division
Faculty Mentor: **Jim Baeder**, UMD Computer Science
Interns: **Philip Charles** (UMD), **Thomas Hamori** (University of South Carolina), **Tak Yeung** (UMD)

TEAM MN: ***Benchmarking Graph Proccessing***
ARLIS Contract Sponsor: DARPA
Faculty Mentors: **Bill Regli**, UMD ARLIS and **Kent O'Sullivan**, UMD
Interns: **Nandini Ramachandran** (UMD), **Morein Ibrahim** (UMD)

TEAM MO: ***Quantum Inspired Classical Computing***
ARLIS Contract Sponsor: DARPA
Faculty Mentors: **Cliston Cole**, Morgan State and **Taylor Paul**, UMD
Interns: **Eliav Hamburger** (UMD), **Jonathan Sharp** (University of South Carolina)

TEAM MS: ***Automated 3D Modeling Improvements***
Champion: NGA Research
Faculty Mentor: **Peter Chang**, UMD Civil and Environmental Engineering
Interns: **Zachariah Davis** (Purdue University), **Alan Luner** (Johns Hopkins University)

TEAM MT: ***Modular, Multi-Lingual Text Extraction Models for Processing, Exploitation, & Dissemination***
Champion: ODNI and Joshua Poore, UMD ARLIS
Faculty Mentor: **Michael Maxwell** and **Shabnam Tafreshi**, UMD
Interns: **Caroline Gish** (Georgetown), **Tejasri Pavuluri** (UMD), **Fei Yang** (UMD Global Campus)

TEAM NE: ***Correlation and Fusion Dashboards for Streaming Data***
Champion: ODNI and Joshua Poore, UMD ARLIS
Faculty Mentor: **Cody Buntain**, UMD
Interns: **Daniel Lamb** (UMD), **Brian Sherwood** (UMD), **Ryan Thenhaus** (University of Wisconsin)

TEAM NH: ***Designing and Implementing an Advanced Machine Learning Technologies in Data Lake Ecosystem for Predicitive Modeling of Chemical Toxicity in the Intelligence Domain***
Champion: US Army Corps of Engineers ERDC
Faculty Mentor: **Jim Purtilo**, UMD Computer Science
Interns: **Vanessa Avelar** (Univ of Texas at El Paso), **Michael Boisclair** (UMD), **Isabella Battish** (UMD)

TEAM NJ: ***Enabling Automated Annotation through User Interaction with Rapid Relabeling***
Champion: ODNI and Joshua Poore, UMD ARLIS
Faculty Mentor: **Jacob Thebault-Spieker**, U Wisconsin
Interns: **Médérick Grivel** (UMD), **Ana Peshku** (UMD), **Musa Waseem** (UMD)

TEAM NM: ***Comparison of North Atlantic Iceberg Detection in Airborne and Satellite Imagery***
Champion: NGA Research
Faculty Mentor: **Deb Niemeier**, UMD
Interns: **James Peng** (UMD), **Emma Vai**l (University of North Georgia)

TEAM NV: ***Data Augmentation of Satellite Imagery to Support Computer Vision***
Champion: NGA Analysis
Faculty Mentor: **Al Cannaday**, University of Missouri
Interns: **Sonrisa Reed** (University of North Georgia), **Emily Massarini** (University of Southern Mississippi), **Breonna Rode**n (University of South Carolina), **Zainab Siddique** (UMD)

TEAM NY: ***Standardizing Pre-Processing & Augmentation for Synthetic Aperture Radar Machine Learning***
Champion: NGA Research
Faculty Mentor: **Chris Metzler**, UMD Computer Science
Interns: **Michelle Gutierrez** (UMD), **Sachin Shah** (UMD)

TEAM NC: ***Building a Convergence Analytical and Planning Tool***
Champion: Fusion OIC, Army G-2
Faculty Mentor: **Alan Fluck**, UMD ARLIS
Interns: **Phillip Ly** (University of North Georgia) and **Ignacio Valdez** (UMD)

TEAM ND: ***Special Warfare PSYOP Training Enhancement with ARLIS Information Competition Simulator***
Champion: 1st Special Warfare Training Group (Airborne)
Faculty Mentor: **Mike Matthaeus**, UMD ARLIS
Interns: **Kyser Daniels-Baessler** (Univ of South Carolina), **Vishwa Ramanakumar** (Univ of Florida)

TEAM OH: ***Civilian perceptions of private and paramilitary groups in contested areas***
Champion: Matt Venhaus, UMD ARLIS
Faculty Mentor: **Meredith Gore**, UMD Georgraphical Sciences with **Brianna Gist**, UMD ARLIS
Interns: **Joseph Coles** (Texas A&M University), **Zachary Einolf** (UMD), **Jonathan Rotman** (UMD)

TEAM OK: ***Applying the Will to Fight to ARLIS Information Competition Simulator***
Champion: III Corps, Army G2
Faculty Mentor: **Matt Venhaus**, UMD ARLIS
Interns: **Alexei Anicheev** (UMD), **Belinda Lin** (UMD)

TEAM OR: ***Information Environment Analysis in the INDOPACOM AOR***
Champion: US Army Pacific Command
Faculty Mentor: **Stan Dubinsky**, University of South Carolina
Interns: **Emilie Reitinger** (Vanderbilt U), **Daniel O'Malley** (Juniata College), **Jonah Benjamin** (UMD)

TEAM PA: ***Diplometrics Data Discovery***
Champion: US Army Pacific Command
Faculty Mentor: **Samuel Henkin**, UMD START
Interns: **Madeline Field** (Seton Hall U), **Aidan Klein** (Indiana University), **Gabriel Paz** (UMD)

TEAM RI: ***U.S. Military Capability Reveal Case Studies***
Champion: Influence & Perception Management, C&SP, OUSD(I&S)
Faculty Mentor: **Ariel Petrovics**, UMD Public Policy
Interns: **Evan Finnessy** (UMD), **Summer Johnson** (Texas A&M University), **Charles Sharp** (UMD)

TEAM SC: ***Did a machine write my homework?***
ARLIS Contract Sponsor: IARPA
Faculty Mentor: **Aric Bills**, UMD ARLIS
Interns: **Nour Ali Ahmed** (UMD), **Sveta Bartholomew** (University of Wisconsin)

TEAM SD: ***Author Personality Trait Classification from Text***
Faculty Mentor: **Triet Le**, UMD ARLIS
Interns: **Ashley Lewis** (Ohio State), **Arjun Chandra**, **Lauren Liberati**, **Pace Ockerman** (UMD)

TEAM TN: ***Communications Trend Targeting***
Champion: ACE SIGENT, Army III Corps G2
Faculty Mentor: **Kaibo Liu**, University of Wisconsin
Interns: **Daniyah Taimur** (UMD), **Joble Thomas** (The Pennsylvania State University Abington)

TEAM TX: ***Synthetic Pattern of Life***
Faculty Mentor: **Pete Loats**, UMD ARLIS
Interns: **Lina Gomez** (UMD), **Laurie Jones** (University of Colorado Boulder), **James van Doorn** (UMD)

TEAM UT: ***Africa's Scientific Landscape***
Champion: AFOSR and Minerva Research Initiative
Faculty Mentor: **David Backer**, UMD Public Policy
Interns: **Adelaide Brooks** (U Iowa), **Elizabeth Dobbs** (U North Georgia), **Elizabeth Arndt** (UMD)

TEAM VA: ***Developing Analytics Critical to Shaping Workforce Enablement & Development Program***
Champion: Security Training, Defense Counterintelligence & Security Agency
Faculty Mentor: **Joe Austerweil**, University of Wisconsin
Interns: **Stephanie Bittle** (Yale), **Jaime Cantwell** (U Glasgow (UK)), **Corinne Guerrero** (Marymount U)

TEAM WA: ***Policy Models for Strengthening STEM Talent Pipeline***
Champion: S&T Program Protection, OUSD(R&E)
Faculty Mentor: **Hassan Salmani**, Howard University
Interns: **James Jenkins** (Univ of North Texas Denton), **Gabriela Schweers** (Harford Community College)

TEAM VT: ***Mining finished intelligence assessments for Crowd-Sourced Forecasting (CSF) use cases***
Champion: Beth Sanner and Neil Wiley, UMD ARLIS
Faculty Mentor: **Mike Dougherty**, UMD Psychology
Interns: **Ethan Ingram** (George Washington U), **Mychala Walker** (UMD), **Madison Dozier** (Marymount U)

TEAM WI: ***Measuring the Quality of Learning from Simulations***
Champion: Directorate of Concepts, Army Futures Command
Faculty Mentor: **Angie Mallory**, UMD ARLIS
Interns: **Lillian Stout** (Princeton University), **Ethan Morrow** (University of Illinois at Urbana-Champaign)

TEAM WY: ***Building infrastructure to faciliate future RISC programs***
Champion: OUSD(I&S)
Faculty Mentor: **David Lovell**, UMD Civil and Environmental Engineering
Interns: **Morgan Smith** (Bowie State University), **Dhruvak Mirani** (UMD)

>> TEAM AL: Risk Framework for Identifying and Protecting Critical Technology RDT&E

GOVERNMENT TOPIC CHAMPION: Office of the Secretary of Defense for Intelligence and Security
RISC FACULTY MENTOR: Eric McGlinchey, George Mason University
RISC INTERNS

- **Lily Bistline**, Loyola University Maryland
- **William Foster**, Georgetown University
- **Gianfranco Secondi**, University of Maryland

PROJECT ABSTRACT

How can we mitigate foreign threats within domestic research institutions in academia and industry without stifling the free and open flow of information and collaboration? Project Alabama addresses this question, in particular focusing on domestic researchers who have been aligned or associated with the government of China. To accomplish this task, we take a data-based approach to observe trends and provide analysis. As such, this project comprises five deliverables.

- A collection of 40 prominent case studies ranging from financial non-disclosure to individuals who commit IP theft on behalf of the Chinese government. Each of these case studies was selected due to prior interest expressed by the US government.
- An interactive map coded in R that visualizes each of the 40 case studies, providing a simplified summary of each case along with relevant information sources.
- A website providing further information for each case study pertaining to context, reporting, and motivations, seeking to expand on the cursory information in the interactive map. The third deliverable is also home to the other deliverables.
- A series of three whitepapers that address: the human motivations surrounding why an individual may want to participate in the TTP or commit an act of IP theft, cyber security risks present in US academia and research institutions and understanding the ties between certain Chinese academic institutions and the PLA.
- An executive summary that synthesizes information from the 40 case studies, evaluates overall data trends from the case studies, summarizes the whitepaper findings, and provides policy recommendations to alleviate this ongoing problem.

Generated resources will help members of the IC to analyze trends and behaviors based on recorded case studies, thereby providing policymakers with valuable information to make informed decisions that will prevent further cases of IP thefts and sensitive data leaks within innovative domestic labs and institutions.

>> TEAM CT: Cybersecurity Vulnerabilities in Critical Infrastructure

GOVERNMENT TOPIC CHAMPION: OUSD (Acquisition & Sustainment) Cyber Warfare
RISC FACULTY MENTOR: Charles Harry, University of Maryland School of Public Policy
RISC INTERNS:

- **Olivia Unzueta**, Pennsylvania State University Dickinson Law
- **Andrew Lee**, Stanford University

PROJECT ABSTRACT

The National Security of the United States is vulnerable to cyber-attacks. The need to secure critical infrastructure that supports operations was underscored by the 2021 Colonial Pipeline hack that significantly disrupted supplies of jet fuel across the East Coast. Cyber-attacks have grown more frequent in the last few years, as military operations have embraced the future of communications technology, incorporating fifth generation cellular communications capabilities and increasing the interconnection of systems to help enable mission sets.

In this work, we present a unified methodology for diagnosing cyber risk to critical infrastructure. We present a scoring metric for quantifying cyber risk, and a software tool that automatically calculates this metric for bases and their supporting commercial critical infrastructure sectors.

LOCATION	COMMUNICATIONS	DIB	ENERGY	GOVERNMENT FACILITIES	TRANSPORTATION	WATER	FOOD AND AGRICULTURE	EMERGENCY SERVICES	FACILITIES
Base 1 Total severity: 64 Organizations: 26 Servers: 31 Open services: 186 Vulnerabilities: 112	**Severity: 51** Organizations: 6 Servers: 6 Open services: 31 Vulnerabilities: 13	**Severity: 18** Organizations: 4 Servers: 6 Open services: 8 Vulnerabilities: 0	**Severity: 52** Organizations: 4 Servers: 4 Open services: 27 Vulnerabilities: 0	**Severity: 42** Organizations: 5 Servers: 5 Open services: 70 Vulnerabilities: 0	**Severity: 22** Organizations: 4 Servers: 7 Open services: 43 Vulnerabilities: 0	**Severity: 51** Organizations: 2 Servers: 2 Open services: 4 Vulnerabilities: 90	**Severity: 66** Organizations: 1 Servers: 1 Open services: 3 Vulnerabilities: 9	N/A	N/A
Base 2 Total severity: 77 Organizations: 27 Servers: 49 Open services: 2483 Vulnerabilities: 448	**Severity: 1** Organizations: 2 Servers: 2 Open services: 15 Vulnerabilities: 0	N/A	**Severity: 1** Organizations: 2 Servers: 2 Open services: 4 Vulnerabilities: 0	N/A	**Severity: 36** Organizations: 3 Servers: 8 Open services: 2368 Vulnerabilities: 0	**Severity: 55** Organizations: 6 Servers: 9 Open services: 20 Vulnerabilities: 34	N/A	**Severity: 70** Organizations: 4 Servers: 12 Open services: 9 Vulnerabilities: 97	**Severity: 78** Organizations: 10 Servers: 16 Open services: 67 Vulnerabilities: 317
Base 3 Total severity: 62 Organizations: 22 Servers: 52 Open services: 339 Vulnerabilities: 109	**Severity: 0** Organizations: 1 Servers: 0 Open services: 0 Vulnerabilities: 0	N/A	**Severity: 61** Organizations: 3 Servers: 8 Open services: 29 Vulnerabilities: 32	N/A	**Severity: 60** Organizations: 4 Servers: 10 Open services: 45 Vulnerabilities: 65	**Severity: 62** Organizations: 8 Servers: 17 Open services: 140 Vulnerabilities: 12	N/A	**Severity: 52** Organizations: 4 Servers: 12 Open services: 81 Vulnerabilities: 0	**Severity: 2** Organizations: 2 Servers: 5 Open services: 44 Vulnerabilities: 0

A chicklet chart visualizing infrastructure exposure for three examined bases (names removed). White and yellow indicate low and moderate exposure, while orange and red indicate severe and very severe exposure.

>> TEAM HI: Unauthorized Installation Access

GOVERNMENT TOPIC CHAMPION: OUSD(I&S) Physical and Operations Security
RISC FACULTY MENTOR: Natalie Scala, Towson University
RISC INTERNS:

- **Noah Hibbler**, University of Maryland
- **Joel Stern**, Brandeis University

PROJECT ABSTRACT

In support of the National Security Strategy, the physical security of Department of Defense (DoD) installations plays a critical role in ensuring the lethality and readiness of our military forces. Attempted and successful Unauthorized Installation Access (UIA), often referred to as breaches and/or gate runners but not just limited to the installation gates, poses a significant threat to the physical security of DoD personnel and resources. While most UIAs are at the installation access points (gates), they also occur at waterside areas, perimeter fences (through jumping, cutting, and digging under), unfenced perimeters, and installation aerial and aquatic boundaries. Despite existing training and physical security measures, UIAs, whether deliberate or not, continue to endanger installations. This raises concerns about the adequacy of current training content and methods, as well as the effectiveness of in-place security measures in deterring UIAs.

To address these issues, we developed an influence diagram to illustrate the complexity and systems nature of the issue, a list of recommended best practices, and a scorecard for identifying the degree of successful implementation of the aforementioned best practices at each installation. Our first step was to visualize the complexity of the problem space. Multiple factors affect a successful or unsuccessful UIA attempt; graphically representing their interconnected nature can help identify redundancies, gaps, and the scale of the problem. OUSD(I&S) has identified multiple systemic problems that we were able to start from. Once the controllable and uncontrollable influences were mapped out, we examined best practices for each of these areas. A significant project outcome was geo-fencing around domestic military installations to notify drivers of restricted usage or private roadways within Google maps. Additionally, there are limited studies regarding the unique position DoD facilities and personnel are subject to, so we adapted recommendations based on other sensitive critical industries as proxies, such as nuclear power and railroads, as well as stressful, physically demanding jobs, such as nursing and law enforcement.

>> TEAM IN: Using Publicly Available Electronic Information to Mitigate Personnel Vetting Failures

SPONSOR: Defense Counterintelligence and Security Agency
RISC FACULTY MENTOR: Harvey Rishikof, UMD ARLIS
RISC INTERNS:

- **Ananya Amirthalingam**, Georgetown University
- **James Maher**, University of Maryland

PROJECT ABSTRACT

Project Horizon is a research project undertaken by ARLIS to provide the Defense Counterintelligence and Security Agency (DCSA) with information on how to improve its use of publicly available electronic information (PAEI) and publicly available social media information (PASMI) in background investigations (BIs) and continuous vetting. Thus far, Project Horizon has conducted research into the laws, regulations, and policies that dictate DCSA's use of PASMI/PAEI and research into PASMI/PAEI data sources, trends, current use by members of the Defense Security Enterprise (DSE), and identity resolution technology.

The specific goal of Team IN has been to supplement the previous research by ARLIS affiliates by creating case studies to be included in the project's final product, to provide DCSA with real examples that highlight how PASMI/PAEI can bolster vetting capabilities and resolve previous investigative gaps. Case studies were selected to represent the diversity of DCSA's workload, and included:

- Mohammad Al-Shamrani Navy Base Shooting in Pensacola
- Involvement of 3 U.S. Marines in Jan 6th Capitol Riot
- Jonathan and Diana Toebbe Submarine Conspiracy
- Pentagon Leaks on Discord (Jack Teixeira and Sarah Bils)
- Ethan Melzer 09A Terrorist Plot

The case studies feature a variety of covered individuals ranging from Defense Industrial Base members to International Military Students to different branches and ranks of U.S. military service members. They also focus on an array of different threats areas such as espionage, dissemination of classified information, terrorism, insurrection, etc. For each case study, we examine whether the presence of PASMI/PAEI in the cases could have prevented or mitigated security failures.

>> TEAM MD: Simulation-Based Verification for Autonomous Systems

SPONSOR: Army Research Laboratory
RISC FACULTY MENTOR: Steven Howell, UMD ARLIS
RISC INTERNS:

- **Tomer Atzili**, University of Maryland
- **Scottie Tran**, University of Maryland

PROJECT ABSTRACT:

The project expanded on testing capabilities surrounding off-road uncrewed ground vehicles (UGV). It is a part of the Simulation-Based Verification and Validation for Autonomous Systems project within the larger AI and Autonomy for Multi-Agent Systems (ArtIAMAS) program, a joint collaboration between the Army Research Laboratory (ARL) and the University of Maryland. Team MD worked to support simulation testing for ARL researchers and their collaborators by expanding, enhancing, and documenting simulation test capabilities. The outcome of this work is accelerated UGV research and development that enables researchers to more thoroughly evaluate UGV use cases in simulation prior to more limited and costly live testing.

This project integrated grass, gravel, and rocky terrain models, test scenes, and related documentation into ARL's UGV simulation environment, enabling researchers to create their own scenes using those terrain models. Team MD leveraged two tools to accomplish this: Unity and Scenic. Unity serves as a 3D modeling software that enables the team to create virtual obstacles or terrain (known as assets). Scenic is a probabilistic programming language that leverages stochastic elements to arrange static and dynamic objects into a scene using declarative programming. The pipeline that the team worked with was to create an asset in Unity, integrate it into Scenic for probabilistic scene creation, then ultimately configure the scenes within Unity. In doing so, the team provided ARL with various terrains that researchers can replicate in real life to test the autonomous control systems of the UGVs. Beyond this, the developed documentation surrounding the project will allow soldiers or researchers to replicate this project's efforts and tailor them for their use case with ease.

>> TEAM NV: Data Augmentation of Overhead Satellite Imagery to Support Computer Vision

GOVERNMENT TOPIC CHAMPION: National Geospatial-Intelligence Agency Research
RISC FACULTY MENTOR: Al Cannaday, University of Missouri Center for Geospatial Intelligence
RISC INTERNS:

- **Emily Massarini**, University of Southern Mississippi
- **Sonrisa Reed**, University of Georgia
- **Breonna Roden**, University of South Carolina
- **Zainab Siddique**, University of Maryland

PROJECT ABSTRACT

Considerable gaps exist in access to the Internet and high-speed mobile coverage, especially in rural areas. Mapping the location of cell phone towers can help improve our understanding of mobile broadband coverage and access which is critical to effective disaster response and our ability to accurately assess and mitigate security threats. While machine learning and satellite imagery have been combined to investigate mobile phone adoption rates in Sub-Saharan Africa (e.g., Oughton and Mathur 2021), there are now efforts, for the first time, to leverage machine learning and computer vision to spatially locate cell towers in rural locations. These efforts will lead to an improvement of cell coverage maps in at-risk regions. Large training datasets are required to train machine learning models. For cell towers that data is often difficult, expensive to collect, or lacks verified locations. Synthetically generated data can supplement real datasets by improving dataset variance and highlighting rare object features.

In this work, Team Nevada developed a low-cost process to rapidly render a large number of synthetic data samples of cell towers on real backgrounds. Delivered products included (1) 500 synthetically rendered data samples with annotations, (2) step-by-step documentation of the rendering process using open-source rendering software Blender, and (3) an extended dataset consisting of an additional 5,100 synthetically rendered data samples not selected for annotation in the project due to time constraint.

>> TEAM OR: Information Environment Analysis in the INDOPACOM AOR

GOVERNMENT TOPIC CHAMPION: U.S. Army Pacific Command
RISC FACULTY MENTOR: Stanley Dubinsky, University of South Carolina
RISC INTERNS:

- **Jonah Benjamin**, University of Maryland
- **Emilie Reitinger**, Vanderbilt University
- **Daniel O'Malley**, University of Pittsburgh

PROJECT ABSTRACT

The University of Maryland's Applied Research Laboratory for Intelligence and Security (ARLIS) has developed the Information Competition Simulator (ICS), a tool that provides a more scientific approach to defense influence operations. The ICS is specifically designed to optimize the use of smaller information samples on a specific target audience's composition, bias, and media consumption patterns. The tool incorporates intelligent software agents with human-like decision parameters and traditional and social media influence mechanisms. The simulator trains its agents through machine learning and artificial intelligence mechanisms derived from social identity theory. ARLIS integrated the ICS into U.S. III Armored Corps (IIIAC) Command Post Exercise (CPX) II in February 2023 and IIIAC's Warfighter Exercise (WFX) 23-4 in April 2023. During these exercises, the ICS was used to model a population in Eastern Europe to measure the effectiveness of influence actions and strengthen the corps' ability to enact the exercise by receiving live feedback and improving response options.

In preparation for a subsequent exercise, ICS will model audiences within the Indo-Pacific Command (INDOPACOM) Area of Responsibility (AOR). This RISC project worked to assist the ICS team with obtaining demographic and psychographic data on focus populations and produced a robust analysis of key media outlets, social media platforms, television stations, and other types of popular media sources. It adopted a holistic perspective to understand socio-political, cultural, and historical phenomena in the studied regions and how these nuances inform present-day biases and media consumption habits.

This effort will inform the information sources used to circulate dissemination materials within the ICS system, directly contributing to the ICS' ability to accurately model the new INDOPACOM AOR populations and their media environments.

>> TEAM RI: U.S. Military Capability Reveal Case Studies

GOVERNMENT TOPIC CHAMPION: Office of the Under Secretary of Defense for Intelligence and Security

RISC FACULTY MENTOR: Ariel Petrovics, University of Maryland School of Public Policy

RISC INTERNS:

- **Evan Finnessy**, University of Maryland
- **Summer Johnson**, Texas A&M University

PROJECT ABSTRACT

Throughout history, both U.S. and adversary militaries have used the reveal or conceal of capabilities, technology, and information in order to advance their respective military and political objectives. The decision to reveal or conceal military capabilities can have great advantages, including strengthening alliances and maintaining strong and effective communication with adversaries. There may also be significant disadvantages including but not limited to, inadvertently false signaling, and potentially destabilizing international agreements which could lead to degrading international relations. Likewise, failure to understand the concept of reveal or conceal as adversaries use it can be disadvantageous.

This project aims to provide stakeholders with an analysis that provides a greater understanding of the reveal or concealment of military capabilities through the use of modern and historical cases and evaluate how this affects U.S. security and political interests. It analyzes two modern examples of reveal or conceal: the Australian-UK-US trilateral security pact (AUKUS), and Russian Disinformation and Conceal Allegations. These modern events were then analyzed against historically illustrative case studies with similar framing.

PHOTO BY LAC AMANDA MCERLICH/U.S. NAVY

The AUKUS agreement showcases a large, multi-faceted, internationally collaborative reveal.

>> TEAM TX: Synthetic Pattern of Life

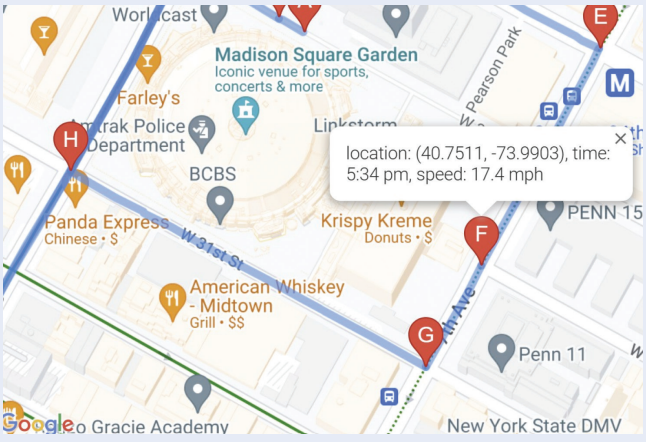
RISC FACULTY MENTOR: Peter Loats, UMD ARLIS
RISC INTERNS:

- **Lina Gomez**, University of Maryland
- **Laurie Jones**, University of Colorado Boulder
- **James van Doorn**, University of Maryland

PROJECT ABSTRACT

The government needs assistance acquiring data for testing systems that evaluate real-world Patterns of Life (POL). Our goal with this project was to lay the groundwork for a comprehensive model generating synthetic and evaluative POL data.

We identified resources that offered a "ground truth" on patterns of human behavior with which we could generate patterns of life data for created synthetic personas. These personas laid a foundation for an initially manually evolving model to a probabilistic random walk model. These models were then accompanied with a routing program that takes the temporally affiliated state-based model output with geospatial locations and routes. This culminates with a comprehensive output that offers a temporal and geospatially described POL dataset. Our deliverable is a generalizable process for creating synthetic POL data that can evolve in complexity.



Snapshot of routing visualization for an example persona with waypoint location, speed, and current time recorded.

>> TEAM WI: Measuring the Quality of Learning from Simulations

SPONSOR: Army Futures Command, Army Concepts Division, Directorate of Concepts
FACULTY MENTOR: Angie Mallory (Maryland)
RISC INTERNS:

- **Lillian Stout**, Princeton
- **Ethan Morrow**, Illinois

PROJECT ABSTRACT:

Wargaming is a form of experimentation often conducted by military organizations to test concepts without the threats and pressures of combat. One important function of wargaming is to help prepare the military for situations that it may face in the future. Senior military leaders use wargame results to make equipment investment decisions, reorganize force structures, suggest new training practices, and more. However, not all wargames are of the same quality. A wargame that is based on flawed premises or poorly executed may yield invalid results. Therefore, it is important that the miliary conducts wargames in valid, rigorous ways. This project, sponsored by Army Futures Command's Futures and Concepts Center, provides recommendations for improving and ensuring the quality of the results achieved through wargaming. The main objective of this work is to create and deliver a Wargaming Process Framework which details a rigorous wargaming process from conceptual development to the reporting of findings. To accomplish this goal, we created a high-level overview of the proposed process and developed each of its stages over the course of the summer. Reference materials, such as evaluation rubrics, and accompanying narratives supplement these stages and serve as a form of standard operating procedure. We hope this work increases the quality of learning from wargames and allows for greater confidence in the changes suggested through experimentation. Ultimately, these recommendations will position future warfighters for success, save lives, and promote the interests of the United States.

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Contact: risc@arlis.umd.edu | 301.226.8900 | www.arlis.umd.edu
7005 52nd Avenue, College Park, Maryland 20742