APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

RESEARCH FOR INTELLIGENCE AND SECURITY CHALLENGES

>> INTERNSHIP PROGRAM / FALL 2024 REPORT

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.

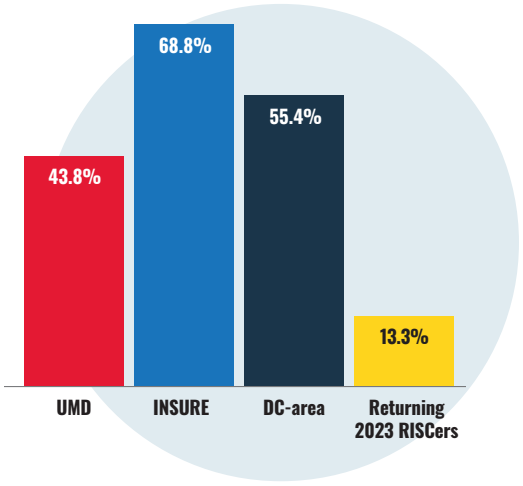
Five years later, the RISC internship program has become a proven model to create and nurture a pipeline of student talent at both graduate and undergraduate levels. The RISC experience provides outstanding students an opportunity to work on real-world problems within ARLIS focus areas as a university-affiliated 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.

WHERE OUR 2024 RISCers COME FROM



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.

"My work here directly correlated to my field of study, allowing me to harden my current skillsets while growing knowledge in new topics at the same time. I now understand different paths into federal government work that I did not realize existed before RISC." –RISC INTERN

2024 INTERN DEMOGRAPHICS

110 interns from **33 institutions** selected from **506 candidates**

79 undergraduates or recent grads

23 MA/MS students

8 PhD/JD students

15 returning interns from RISC 2023

19 interns from HBCU / MSI schools

77 interns from INSURE consortium universities

50 from outside the National Capital Region

Each year evaluators consider a talented applicant pool to identify RISC interns. Candidates are assessed on 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 and seniors and early graduate students–are eligible and encouraged to apply.

Disciplines of Interest

Specifically, the RISC initiative has 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 systems 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: Measurement and evaluation of learning outcomes, environmental modeling and remote sensing, human factors, and regulatory public policy.

"I am beyond grateful that I had the opportunity to be a part of this program. I learned so much–not just about my topic but about working a full-time job with real stakes, responsibility, working as part of a time, IC writing, presenting, and so much more. This was the first experience I've had where I have truly felt like I was making a difference and impacting at least a small part of the world." –RISC INTERN

Interns, mentors, ARLIS researchers, and government stakeholders attended the 2024 RISC Research Showcase to be briefed on project outcomes.

In 2024, ARLIS received applications from 506 candidates from 115 universities and 110 students were selected from 33 universities. The students selected for RISC 2024 brought backgrounds including:

- **Applied Mathematics** and **Statistics**
- **Area Studies** and **Languages** (22 with significant foreign language expertise)
- **Computer Science** and **Engineering**
- **Criminology**
- **Economics**
- **Geographical Sciences**
- **Industrial Engineering**
- **Information Science**
- **Cybersecurity**
- **Cryptography**
- **Psychology** and **Sociology**
- **Security Studies**
- **Public Policy** & **International Relations**

Hannah Haber (University of Maryland) and Donovan Decker (Texas A&M) brief a government stakeholder on their project work.

Intern Alexandra Bogle (The Pennsylvania State University) talks with an HR representative from the National Geospatial Intelligence Agency during the Reverse Career Fair held in parallel with the Research Showcase.

"This summer has underscored for me that ARLIS is a great place to work. People have been incredibly kind, gracious, and willing to share/learn new things. I now know that I seek a work environment similar to this one."

–RISC INTERN

"This is my third year with the program, and it is a lot of fun to see the students tackle a problem and grow professionally during the summer" –RISC MENTOR

The class of 2024 supported 46 projects benefiting 25 defense and intelligence agencies and offices. 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 guidelines.
- Examining responsible ways to incorporate AI into missions.
- Conducting test and evaluation for a service to improve interactions with international audiences.

Project abstracts from 10 of these 46 projects are included in this report, representative of the wide range of problems tackled.

RISC 2024 PROJECT TYPE	% OF PROJECTS
AI/ML programming	20%
Case studies	1.33%
Data science/stats	8.67%
Language and linguistics	1.33%
Literature reviews	6.67%
Open-source intelligence	8%
Policy	10%
Programming, but not AI/ML	12%
Qualitative analysis	20.67%
Simulations and wargaming	4%
SME interviews	2%
System design	2%
Test and evaluation	3.33%

The RISC Experience

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

The program is structured to facilitate interactions within teams, between teams, and with government sponsor representatives. Interns attended weekly seminars and regular team development meetings in a shared virtual work environment, although select projects 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 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. As of September 2024, 45 interns from summer 2024 were continuing to work with ARLIS for the academic year.

"I learned more about different technical skills that I had absolutely no background in and it made me realize what paths I truly wanted to follow."

–RISC INTERN

"My career options have significantly widened, I have so many new people to network with and contact now." –RISC INTERN

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 Department of Defense;
- ethical, legal and social implications of AI and technology in warfare;
- using the presidential daily briefing as an example of how to present effectively;
- law enforcement intelligence and domestic security;
- I&S roles focusing on strategic competition;
- cyber operations in the military; and
- considering careers in the civilian government sector.

Interns Asmita Brahme and Saanvi Kataria (both University of Maryland students) brief ARLISans and government representatives on their analysis of "Cloud-Based Portals for Quantum Compute Systems."

Faculty mentors engage ARLIS Government Program Manager Greg Weisler to better understand how the summer projects they supported tied to government challenges.

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. These faculty mentors work with the government topic champion translate a mission-relevant problem into a project scoped to generate actionable outcomes over the short 10-week program period.

In 2024, 50 mentors supported the 46 projects, with 18 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. 34 mentors returned from prior RISC programs, providing their previous talents and insights for ARLIS to engage for future intelligence.

University of Maryland faculty mentors outside of ARLIS came from UMD's School of Public Policy, College of Information Studies, and the Departments of Geographical Sciences, Computer Science, Civil & Environmental Engineering, Psychology, and the Center for the Study of Terrorism and Reactions to Terrorism.

RISC 2024 interns, mentors and program team.

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 2024, ARLIS had the privilege to work with USG topic champions representing over 25 distinct organizations within the defense intelligence and security enterprise:

Undersecretary of Defense for Intelligence and Security - core sponsor
- Counterintelligence, Law Enforcement, & Security
- Sensitive Activities and Special Projects

OUSD(Research & Engineering)
- S&T Program Protection
- Maintaining Tech Advantage
- Basic Research Office/Minerva

OUSD(Acquisition & Sustainment)
- Office of the Chief Information Security Officer/Cyber Warfare
- Defense Operational Test & Evaluation

National Geospatial-Intelligence Agency

Intelligence Advanced Research Projects Activity

Central Intelligence Agency

Army
- PEO Intelligence, Electronic Warfare & Sensors
- Army Research Lab
- Army Research Office
- III Armored Corps G2/SIO
- 1st Special Warfare Training Group

Air Force
- Office of Scientific Research
- AFOSI Defense Cyber Crime Center

Navy
- Naval Air Warfare Center
- Naval Undersea Warfare Center

Defense Technical Intelligence Center

ARLIS projects from **DARPA**, **ONR**, **DCSA**, **IARPA** and elsewhere

"RISC 2024 has greatly improved my own personal clarity and direction with wanting to pursue a career in the intelligence field."

–RISC INTERN

"I was immensely impressed by both of the interns that I mentored. Together with the great interns I mentored last year, this speaks to the quality of the selection process."

–RISC MENTOR

"RISC 2024 created an environment where I applied textbook concepts to real-world issues. Participating in this internship provided me the opportunity to further develop my skill set, becoming a more attractive applicant to the Intelligence Community" –RISC INTERN

"Working together with equally-ambitious mentors and interns allowed me to foster valuable career connections that I intend to use closer to graduation."

–RISC INTERN

"I would encourage others to apply for the networking opportunities and the chance to learn about paths into the federal government. Just hearing about the many ways people got involved (and the number of people saying they "stumbled into the field") made me much more confident in the possibilities with the government." –RISC INTERN

ARLIS engineer John Romano served as one of the Research Showcase judges, here talking to interns Adji Diouf (Howard University) and Lauren Hobson (George Mason University) about their work classifying supply chain vulnerabilities. Top scoring project teams had the opportunity to brief senior DoD and Intelligence Community representatives at the closing events.

Metrics of Success

RISC has grown a lot since its inception, from a small lab internship (17 students) in 2020 to a major national program (110 students) in 2024. A large majority of the interns have expressed a desire to pursue careers in intelligence and security. The program now boasts over 370 alumni, around 75% having graduated and entered the workforce.

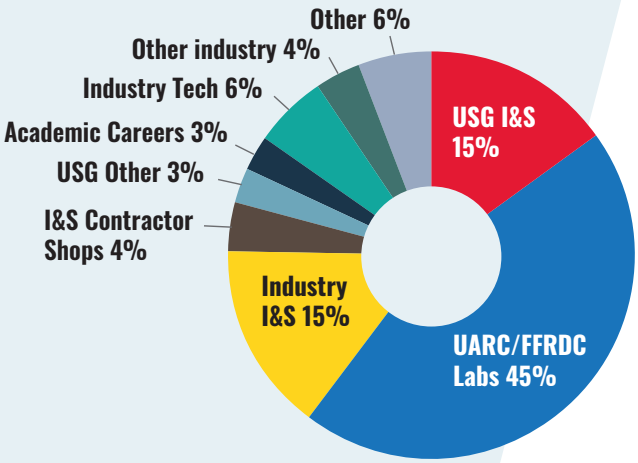
From 2022 through September 2024, 306 RISC interns have been positively adjudicated for security clearances. These clearances help facilitate RISCer career paths while also augmenting the credentialed talent pool for the intelligence and security communities.

Program Outcomes

As a workforce development program geared towards increasing student interest in Defense, Intelligence, and Security careers, we are excited to show that the majority of our interns are pursuing intelligence and security careers. This year, more than 40% of summer interns opted to continue supporting ARLIS research projects into the academic year. As of 2024, many past interns are still students, but of those who have moved on to full-time careers, the majority are working in support of the U.S. government either directly as Intelligence and Security employees, Intelligence and Security contractors, at SETA shops, or at UARCS/FFRDCs.

Ahead, the RISC Planning Team is working with senior government human resources executives to find ways to increase the number of RISCers taking jobs in the federal workforce directly. This includes working to clarify the direct hiring authorities used by agencies to hire their own interns, with the goal of also directly hiring successful RISC interns.

WHERE RISCers GO



"RISC was a fantastic experience. It solidified my desire to work in the [Intelligence Community] after graduation and the experience it gave me was extremely helpful when I applied for government positions."

–RISC INTERN

"I am now considering the IC as a potential career path where before [RISC] I wouldn't have."

–RISC INTERN

"Government based work genuinely interests me now, unlike before when I put it off as unserious busy work. There are genuine impacts and benefits to working with the government, especially the IC." –RISC INTERN

RISC: 2024 PROJECTS

TEAM AK: *Exploring Generative AI for Metadata Creation in Records Management*

Faculty Mentors: **Michael Brundage**, **Amir Ghaemi**, **Jennifer Proctor** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Rena Max** (University of Maryland), **Steven Su** (University of Maryland)

TEAM AL: *Computer Vision: Image Detection Leveraging Un-labeled Data*

Champions: Laurence Mixon (Army PEO IEWS), Bharat Patel (Army PEO IEWS)
Faculty Mentor: **Al Cannaday** (University of Missouri)
Interns: **David Zikel** (University of Wisconsin – Madison), **Michael Boisclair** (University of Maryland)

TEAM AR: *Cloud-Based Portal for Quantum Compute Systems*

Champion: Paul Lopata (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentors: **Allison Casey** (UMD Applied Research Laboratory for Intelligence and Security), **Darrell Teegarden** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Asmita Brahme** (University of Maryland), **Kataria Saanvi** (University of Maryland)

TEAM AZ: *Simulation-Based Verification for Autonomous Systems*

Champion: Craig Lennon (Army Research Laboratory)
Faculty Mentor: **Steven Howell** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Nadia Meyerovich** (University of Maryland), **Kevin Pham** (University of North Texas)

TEAM CA: *Streamlining Document Triage with Advanced LLM Capabilities*

Champion: Joshua Poore (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentors: **Alan McMillan** (University of Wisconsin), **Alex Walter-Higgins** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Cheyenne Bajani** (George Mason University), **Glenn Fitzpatrick** (Texas A&M University), **Arjun Iyer** (University of Virginia)

TEAM CO: *Retrieval-Augmented Generation (RAG) Pipeline Capabilities for Better Data Exploitation*

Champion: Anthony P. (ODNI)
Faculty Mentor: **Ramani Duraiswami** (UMD Computer Science)
Interns: **Drew Galbraith** (Brigham Young University), **Mouhmadou Hoyek** (Howard University), **Ashby Steward-Nola**n (Smith College)

TEAM CT: *Connections 2.0*

Champion: Tim Sprock (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Amanda Chicoli** (University of Maryland)
Interns: **Fouad Ayoub** (University of Maryland), **Nihal Garisa** (University of Maryland), **Dhruvak Mirani** (University of Maryland), **Peter Smith** (University of Maryland)

TEAM DC: *Enhancing Software T&E through Full-Stack Instrumentation*

Champion: Joshua Poore (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentors: **Evan Jones** (UMD Applied Research Laboratory for Intelligence and Security), **Alex Walter-Higgins** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Jackson Hitzeman** (University of Wisconsin), **Breonna Roden** (University of South Carolina)

TEAM DE: *Computational Models of Cognitive Error*

Champion: Kimberly Ferguson-Walter (IARPA)
Faculty Mentor: **Ruthanna Gordon** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Maia Lenes** (University of Maryland), **David Peabody** (Texas Tech)

TEAM FL: *Meaningfulness in Life in Relation to Social and Political Sentiments*

Champion: Victor Frank (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Sharon Glazer** (University of Baltimore)
Interns: **Alaina Fletcher** (Virginia Tech), **Jason Grove** (University of Maryland)

TEAM GA: *Geographic Distribution of U.S. Innovation*

Champions: Robert Irie (OUSDRE-STPP), Chris Nissen (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **David Backer** (University of Maryland)
Interns: **Emily Bogle** (Penn State University), **John Derks** (University of Maryland), **Huimin Lin** (University of Maryland)

TEAM HI: *The Nexus of Academic Openness, Collaborative Ventures, and National Security Imperatives*

Champion: Robert Irie (OUSDRE-STPP)
Faculty Mentor: **Christopher Nissen** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Robert Hopkins** (University of Maryland), **Vyas Kepler**, (University of Maryland), **Orsola Tragni** (Louisiana State University)

TEAM IA: *Expanding Vulnerability Disclosure Programs for the Defense Industrial Base*

Champion: John Repici (AFOSI DC3)
Faculty Mentors: **Kelly Giraud** (UMD Applied Research Laboratory for Intelligence and Security), **Brett Berlin** (GMU)
Interns: **Shameer Rao** (Morgan State University), **Sydney Weinstein** (American University)

TEAM ID: *The Role of Platforms in Driving the Rate of Technical Innovation & Invention*

Champions: Robert Irie (OUSDRE-STPP), Chris Nissen (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Zachary Boyd** (Brigham Young University)
Interns: **Janneth Najera** (Texas A&M), **Samuel Park** (Texas A&M)

TEAM IL: *Attack Surface Mapping of Base Critical Infrastructure*

Champion: Ken Wang (OUSDA&S CWD)
Faculty Mentor: **Charles Harry** (University of Maryland)
Intern: **Akash Bhave** (University of Maryland)

TEAM IN: *Cyber Tools: Intrusion Detection Systems to Safeguard Vehicles*

Champions: Jordon Adams (DOTE), Juliana Ivancik (DOTE)
Faculty Mentor: **Hassan Salmani** (Howard University)
Interns: **Andino LaVersa** (Howard University), **Ilan Shefi** (SUNY Albany), **Rachel Wang** (George Mason University)

TEAM KS: *Did a Machine Write My Homework?*

Champion: Anton Rytting (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Aric Bills** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **James Crews** (University of South Carolina), **Jared Suchomel** (Brigham Young University)

TEAM KY: *Doctrinal Language Detection*

Champions: Erik Nesse (UMD Applied Research Laboratory for Intelligence and Security), Henry Overos (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Isaac Gang** (George Mason University)
Interns: **Konstantine Kahadze** (University of Maryland), **Elizabeth Kemp** (University of Florida)

TEAM LA: *Narrative Change in Discursive Contexts*

Champions: Erik Nesse (UMD Applied Research Laboratory for Intelligence and Security), Henry Overos (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Stanley Dubinsky** (University of South Carolina)
Interns: **Elena Jaimes** (University of Maryland), **Tony Ventura** (SUNY Albany)

TEAM MA: *Investigating and Re-tuning the OODA Loop*

Champion: Laura Steckman (AFOSR)
Faculty Mentor: **Cody Buntain** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Claire Holmes** (Carleton College), **Michael White** (Texas A&M)

TEAM MD: *Best Practices and Future Directions in Human Systems Integration*

Champion: Stephanie Proule (Navy NUWC)
Faculty Mentors: **Melissa Carraway** (UMD Applied Research Laboratory for Intelligence and Security), **Kelley Gunther** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Emily Hewitt** (Marymount University), **William Lewis**, (Brigham Young University), **Tali Schlenoff** (University of Maryland)

TEAM ME: *Analysis of International Communication on the Topic of Quantum Computing*

Champion: Paul Lopata (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Angie Mallory** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Alexandra Bogle** (Penn State University), **Katherine Donovan** (Hamilton College)

TEAM MI: *User Interface (UI) Programming and Game Design for Information Competition Simulator (ICS)*

Champion: Matt Venhaus (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentors: **Nurul Haya** (UMD Applied Research Laboratory for Intelligence and Security), **Matt Venhaus** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Victoria Liu** (University of Maryland), **Suhan Neema** (University of Maryland)

TEAM MN: *Extracting Emotional Content to Establish Emotional Pairings Between Online Discussants*

Champions: Gregory Ruark (Army ARO), Matt Venhaus (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Amanda Hughes** (Brigham Young University)
Interns: **Quinn Bruce** (University of Wisconsin), **Peyton Lutchkus** (Robert Morris University), **Niobe Melendy** (Hofstra University)

TEAM MO: *Modeling and Mapping the Will to Fight of Foreign Militaries*

Champion: Matt Venhaus (AR UMD Applied Research Laboratory for Intelligence and Security LIS)
Faculty Mentor: **Timothy Clancy** (University of Maryland)
Interns: **Joseph Coles** (Texas A&M), **Madeline Field** (Seton Hall University), **Jonathan Rotman** (University of Maryland)

TEAM MS: *Development of Software-Based Agents Using the Hierarchy of Psychological Effects Model*

Champion: Marty Bartram (Army Special Warfare Center)
Faculty Mentor: **Mike Matthaeus** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Avery Kops** (University of Maryland), **Bennett Sellers** (University of Maryland)

TEAM MT: *Wargaming Ethnography*

Champion: Jean Luc Cambiar and David Montgomery (OUSDRE-BRO)
Faculty Mentors: **Michaela Gawrys** (University of Maryland), **Madeline Romm** (University of Maryland)
Interns: **Alana Ackerman** (University of Illinois), **Isabelle Antonetti** (University of Maryland), **Jessica Hill** (American)

"Our program/project sponsor was gushing during a meeting about how impressed they were with the program and the students! One comment was, 'these undergraduate students were more poised and capable than many of the college graduate professionals I work with...." –RISC MENTOR

TEAM NC: *Mapping and Assessing Intellectual Property Protection Policy and Regulation*

Champion: Robert Irie (OUSDRE-STPP)
Faculty Mentor: **Wendi Kaspar** (Texas A&M)
Interns: **Katherine Lehner** (Virginia Tech), **Gregory Peng** (University of Illinois), **Hayley Schneider** (University of Maryland)

TEAM ND: *Understanding Generational Perspectives on "Need to Know"*

Champion: Michael Russo (OUSDIS-CLS-ISD)
Faculty Mentor: **Gary Brown** (Texas A&M)
Interns: **Autumn Perkey** (University of Maryland), **Ella Reid** (University of North Georgia), **Laura Short** (University of Pittsburgh)

TEAM NE: *Artificial Intelligence in Malware Processing*

Champion: Kevin Rivera (AFOSI DC3)
Faculty Mentor: **Cliston Cole** (Morgan State University)
Interns: **Clinton Kobe** (University of Maryland), **Alexandre Robic** (Texas A&M)

TEAM NH: *Linked Data Annotation for Declassification*

Faculty Mentors: **Michael Brundage** (UMD Applied Research Laboratory for Intelligence and Security), **Amir Ghaemi** (UMD Applied Research Laboratory for Intelligence and Security), **Jennifer Proctor** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Svetlana Bartholomew** (University of Wisconsin), **Angela Boley** (University of Maryland), **James van Doorn** (University of Maryland)

TEAM NJ: *Enhancing the DoD's Operational Planning with LLMs through Rigorous T&E*

Champion: Joshua Poore (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentors: **Evan Jones** (UMD Applied Research Laboratory for Intelligence and Security), **Christopher Metzler** (University of Maryland), **Alex Walter-Higgins** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Kyle Huang** (University of Wisconsin), **Jugraj Singh** (University of Maryland)

TEAM NM: *Reducing Compliance Burden on Small Businesses*

Champion: Yvette Jacks (DTIC)
Faculty Mentor: **Kaibo Liu** (University of Wisconsin)
Interns: **Chamarr Auber** (University of Maryland), **Billy Battles** (George Mason University)

TEAM NV: *Artificial Intelligence Risk Evaluation Framework*

Champions: Laurence Mixon (Army PEO IEWS), Bharat Patel (Army PEO IEWS)
Faculty Mentor: **Jim Purtilo** (University of Maryland)
Interns: **Tomer Atzili** (University of Maryland), **Joey Kim** (University of Maryland), **Smit Patel** (University of North Georgia)

TEAM NY: *Navigating the Regulatory Landscape: Impact on Biotechnology*

Champions: Lauren Quattrochi (OUSDRE-STPP-MTA), A. Cody Youngbull (OUSDRE-STPP-MTA)
Faculty Mentor: **Michelle Bensi** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Harrison Hill** (University of Maryland), **Sydney Mason** (George Mason University)

TEAM OH: *Human Accountability in Off-the-Loop Autonomous Systems*

Faculty Mentors: **Lauren Diaz** (UMD Applied Research Laboratory for Intelligence and Security), **Harvey Rishikof** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Brandon Dang** (University of Maryland), **Allison Diveley** (University of Maryland)

TEAM OK: *Country-wide Overviews on China's International Economic and Business Interests*

Faculty Mentors: **Evan Ream** (UMD Applied Research Laboratory for Intelligence and Security), **Tim Sprock** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Madeline Bagdade** (Brandeis University), **Robert Schantz** (Texas A&M), **Isaac Weber** (Patrick Henry College)

TEAM OR: *Military Coups in West and Central Africa*

Champion: Brianna Gist (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Eric McGlinchey** (George Mason University)
Interns: **Kaitlyn DaVisio** (American University), **Mouhamadou Hoyeck** (Howard University), **Emma O'Horo** (College of William & Mary)

TEAM PA: *AI/ML to Support Defense Security Policy*

Champion: Amanda McGlone (OUSDIS-CLS)
Faculty Mentor: **Allison Reilly** (University of Maryland)
Interns: **Isabella Battish** (University of Maryland), **Preethi Pai** (University of Maryland)

TEAM RI: *Sensor Network Design for Airborne Chemical Monitoring and Prediction*

Champion: A. Cody Youngbull (OUSDRE-STPP-MTA)
Faculty Mentor: **Steve Sin** (University of Maryland)
Interns: **Emmelia Cieslewicz** (Brigham Young University), **Anh Nguyen** (Texas A&M)

TEAM SC: *Comparison of North Atlantic Iceberg Detection in Airborne and Satellite Imagery*

Champion: Rachel Bernstein (NGA)
Faculty Mentor: **Deb Niemeier** (University of Maryland)
Interns: **Eliav Hamburger** (University of Maryland), **Guang-Lin Wei** (University of Maryland)

TEAM SD: *Reducing Erroneous ML Observations Through Topological Reasoning*

Champion: Michael Lenihan (NGA)
Faculty Mentor: **Paulo Shakarian** (Arizona State University)
Intern: **Edward Wang** (Johns Hopkins University)

TEAM TN: *Industrial Security Risk Calculus*

Champion: Tim Sprock (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Natalie Scala** (Towson University)
Interns: **Shreenidhi Ayinala** (University of Maryland), **Navya Gautam** (University of Maryland)

TEAM TX: *Identifying and Classifying Supply Chain Vulnerabilities*

Champion: Tim Sprock (UMD Applied Research Laboratory for Intelligence and Security)
Faculty Mentor: **Meredith Gore** (University of Maryland)
Interns: **Adji Diouf** (Howard), **Lauren Hobson** (George Mason University), **Carter Linke** (University of South Dakota), **Mason Meinzinger** (Embry-Riddle Aeronautical University)

TEAM UT: *Defense Industrial Base*

Champion: OUSDIS-CSP
Faculty Mentor: **Tim Sprock** (UMD Applied Research Laboratory for Intelligence and Security)
Interns: **Donovan Decker** (Texas A&M), **Hannah Haber** (University of Maryland)

TEAM VT: *Understanding Malicious Cyber Actors' (MCA) Synthetic Influence Operations*

Champion: Elizabeth Niedbala (NSA R2)
Faculty Mentor: **Jason Spitaletta** (National Intelligence University)
Interns: **Jeffrey Cole** (University of Maryland), **Sydney Lynch** (University of Mississippi)

"I truly enjoyed the mentoring experience and seeing the projects come to life on the last days." –RISC MENTOR

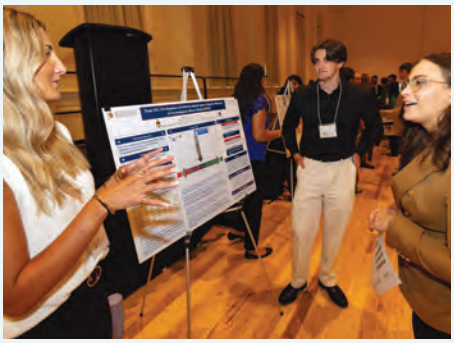
"My project area was not something I was at all familiar with, or frankly cared about, before the summer. But now, I could genuinely be considered knowledgeable in this very niche field of research, and I am considering ways to integrate it into my further career."

–RISC INTERN

Alana Ackerman (University of Illinois, Urbana-Champaign) discusses her project with Evan Jones (ARLIS), Devin Ellis (ARLIS), and Meghan Hersh (ARLIS).



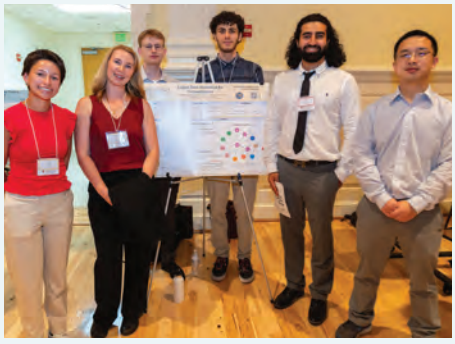











PHOTOGRAPHY BY RILEY N. SIMS/UNIVERSITY OF MARYLAND

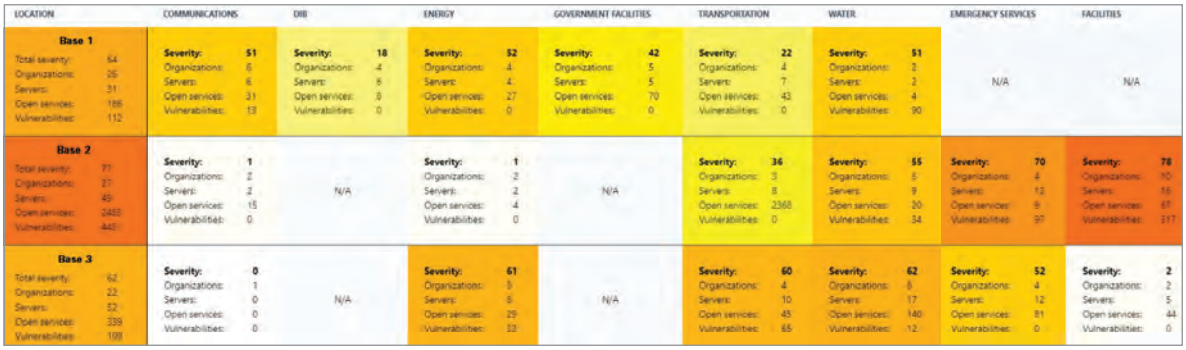
>> TEAM CT: Cybersecurity Vulnerabilities in Critical Infrastructure

GOVERNMENT TOPIC CHAMPION: OUSD (Acquisition & Sustainment) Cyber Warfare
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**

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.



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.

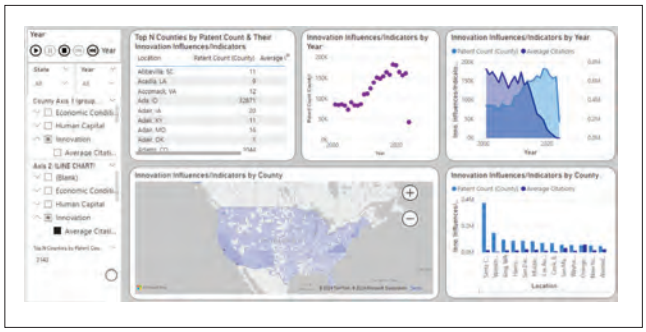
>> TEAM GA: Geographic Distribution of U.S. Innovation

GOVERNMENT TOPIC CHAMPION: Robert Irie (OUSDRE-STPP)
FACULTY MENTOR: David Backer
RISC INTERNS:

- Emily Bogle
- John Derks
- Huimin Lin

PROJECT ABSTRACT

Our project aims to provide a thorough understanding of the U.S. innovation landscape, focusing on uncovering the potential of overlooked areas alongside more established regions. We are developing two main products: (1) an interactive data dashboard that offers a detailed view of measures of innovation and associated factors at both state and county levels, and (2) a report that includes an overview of foundational literature, a summary of patterns and trends of innovation over the last 20-25 years, an examination of significant influences on innovation, and (if possible) forecasts of the future trajectory of innovation.



Screenshot of Project Interactive Data Dashboard

A detailed appreciation of the U.S. innovation landscape is crucial to the U.S. Government (USG) – and the U.S. Department of Defense (DOD) in particular – for purposes of maintaining a competitive technological edge and safeguarding technology leadership. This awareness will help our sponsor and other key stakeholders build and capitalize on strengths, pursue existing and emergent opportunities, make informed and effective investments, and mitigate weaknesses and threats. An ultimate intention of the project is to ensure the reliability, integrity, accessibility and resilience of U.S. technology frameworks in fulfilling strategic interests of the USG and DOD.

To achieve these objectives, our workflow involves several primary tasks. The starting place is consolidating available literature to establish how the concept of innovation is defined and studied. Next, we are identifying and acquiring statistical data from multiple sources, encompassing more than 40 indicators. We are then processing (cleaning, merging, etc.) this data using Python and R, resulting in a cohesive master sheet that serves as the backbone for analysis. In particular, we are developing an interactive data dashboard in Power Bi to visualize the spatio-temporal patterns and trends of both indicators of innovation and factors of interest. Finally, we will conduct bivariate and multivariate analysis using R to investigate the relationship between various innovation indicators and factor variables, allowing us to pinpoint key drivers of innovation and their interactions.

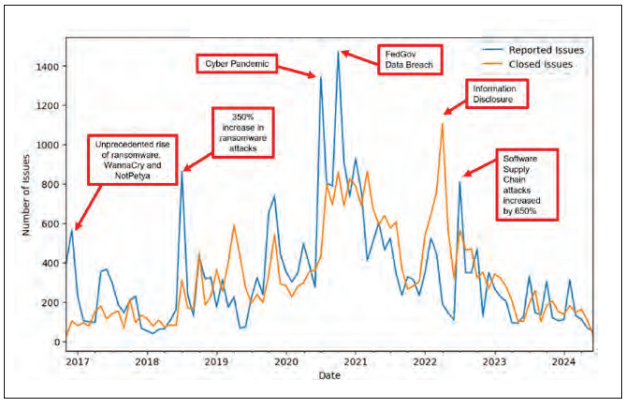
>> TEAM IA: Expanding Vulnerability Disclosure Programs for the Defense Industrial Base

GOVERNMENT TOPIC CHAMPION: John Repici (AFOSI DC3)
FACULTY MENTORS: Brett Berlin and Kelly Giraud
RISC INTERNS

- Shameer Rao
- Sydney Weinstein

PROJECT ABSTRACT

Team IA aims to produce products that will inform the growth and development of DC3's Vulnerability Disclosure Program (VDP) and the Defense Industrial Base VDP (DIB-VDP). With the demand for vulnerability management in the Department of Defense (DoD) growing faster than the existing VDP programs, the RISC team will create four comprehensive products to address this challenge. These products will investigate the VDP landscape through data exploration, providing valuable insights for future researchers and participants.



Monthly Reported and Closed Issues

The first product, a Framework, will offer high-level methodologies, tools, and best practices for VDP researchers. The second product, an Educational Toolkit, will equip students and educators with essential VDP skills. The third product, a Trend Analysis, will identify trends in VDP tools and methodologies. The fourth product, Forward Vision, will examine current legislation and policies to project the future of VDP programs within the DoD.

DC3's VDP and DIB-VDP programs have been crucial in enhancing DoD and national security by addressing tens of thousands of exploitable vulnerabilities annually at a low cost. Our project aims to create tools that will develop a highly qualified workforce, investigate current reports, and identify the most critical vulnerabilities. This will increase the number of skilled federal employees securing the government.

Through background research, data cleaning, flexible outlining, and continuous collaboration with sponsors and mentors, Team IA will ensure the successful completion of these products. The outcomes will meet the current needs of the VDP and explore the potential for scaling these programs, addressing how ongoing legislative efforts might impact the DIB-VDP and the broader VDP landscape.

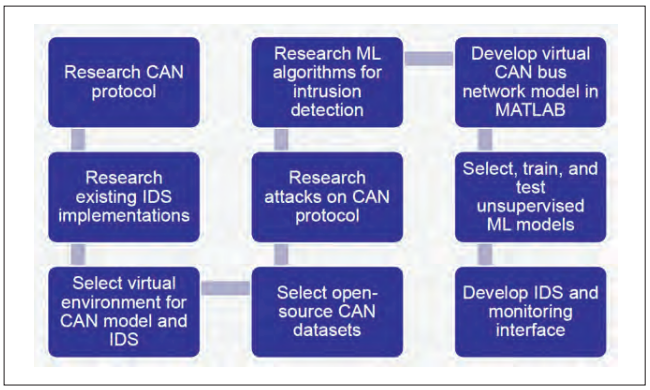
>> TEAM IN: Cyber Tools: Intrusion Detection Systems to Safeguard Vehicles

GOVERNMENT TOPIC CHAMPIONS: Jordon Adams (DOTE), Juliana Ivancik (DOTE)
FACULTY MENTOR: Hassan Salmani
RISC INTERNS

- Andino LaVersa
- Ilan Shefi
- Rachel Wang

PROJECT ABSTRACT

Today's increasingly complex and networked systems present challenges in determining the occurrence of a cyber-attack. Detection is even more challenging on vehicles and against cyber-attacks with no apparent changes to the system, necessitating tools that can continuously monitor systems to detect cyber-attacks as soon as they occur. One such tool is a reliable, real-time intrusion detection system (IDS) to safeguard vehicles against various threats and attacks targeting the Controller Area Network (CAN) bus network. Project IN aims to address this need through the development of a real-time IDS that first monitors CAN traffic and establishes a system baseline to later flag anomalous CAN traffic as potential cyber-attacks.



Project overview. CAN: Controller Area Network; IDS: Intrusion Detection System

Team IN will accomplish this objective by (1) researching the Controller Area Network (CAN) protocol, its associated vulnerabilities and potential attacks, and existing approaches to IDS development for CAN bus security; (2) designing, developing, and testing a functional IDS solution prototype (CANGuard) that uses machine learning models to detect threats to vehicle CAN bus infrastructure; (3) developing a runtime monitoring interface for the IDS prototype, and (4) creating relevant user guides and documentation. These efforts will provide an accurate and effective monitoring system to better secure vehicles and CAN bus networks against current, emerging, and future threats.

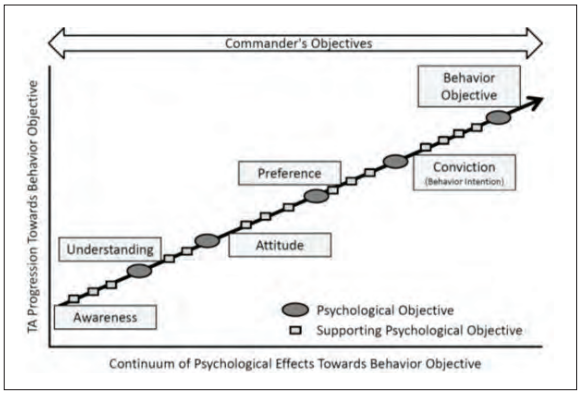
>> TEAM MS: Development of Software-Based Agents Using the Hierarchy of Psychological Effects Model (HPEM)

GOVERNMENT TOPIC CHAMPION: Marty Bartram (Army Special Warfare Center)
FACULTY MENTOR: Mike Matthaeus
RISC INTERNS:

- Avery Kops
- Bennett Sellers

PROJECT ABSTRACT

The development of software-based agents using the hierarchy of psychological effects model (HPEM) is an abstract project that involves the implementation of the HPEM framework into Information Competition Simulator (ICS) agents. The purpose and goal of this project is to improve war-gaming, military training, and Psychological Operations (PSYOP) activities by creating a more realistic agent population whose actions are guided by a psychological model that reflects human behavior. Ultimately our implementation aims to establish a strong connection between the ICS and Psychological Operations doctrine. To achieve this goal, we drafted and revised several potential frameworks, met with several ICS team members, researched translational models, and analyzed the NetLogo code on which the simulation runs on. Additionally, we plan to run the current framework through ICS and revise as necessary to implement the most accurate portrayal of HPEM and human behavior into the ICS agents.



Hierarchy of Psychological Effects Model Hierarchy of Psychological Effects Model

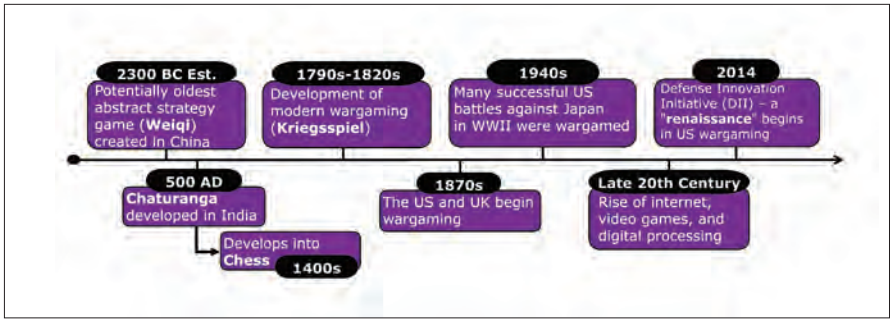
>> TEAM MT: Wargaming Ethnography

GOVERNMENT TOPIC CHAMPION: David Montgomery (OUSDRE-BRO)
FACULTY MENTORS: Michaela Gawrys, Madeline Romm
RISC INTERNS:

- Alana Ackerman
- Isabelle Antonetti
- Jessica Hill

PROJECT ABSTRACT

To bolster the next generation of wargaming, materials and best practices must be drafted after a critical analysis of prior iterations. This project synthesizes and analyzes historic and contemporary literature as well as formal United States (U.S.) and United Kingdom (U.K.) handbooks to create a literature review which will be used to support a thorough ethnography of wargaming. This ethnography is task 3 of 4 in an overarching ARLIS project for the Asymmetric Threat Analysis Center (ATAC) with the ultimate objective of developing a model to improve the fundamental science of wargaming and integrate those improvements into the wargaming community. The focused goal of the ethnographic report is to deepen the understanding of the sociocultural dynamics of wargaming and how technological shifts have historically impacted wargames. By analyzing both the expected and experienced spaces, this ethnography will identify opportunities and constraints on how a new model is likely to be received and adopted.



The Evolution of Wargaming

>> TEAM ND: Understanding Generational Perspectives on "Need to Know"

GOVERNMENT TOPIC CHAMPION: Michael Russo (OUSDIS-CLS-ISD)
FACULTY MENTOR: Gary Brown
RISC INTERNS:

- Autumn Perkey
- Ella Reid
- Laura Short

PROJECT ABSTRACT

A valid "need to know" (NTK) is one of the three requirements for access to classified information. A review directed by the Secretary of Defense indicated that managing NTK at scale is difficult and often subjectively assessed. A younger generation is entering the national security workforce, social media use is rising, and the national security community is increasing its use of digital tools, this study aims to determine the effect of these trends on the understanding of NTK. The methodology employed includes a literature review of the law and policy surrounding NTK; research-based development of meaningful definitions of various generations of the workforce; development and administration of a novel survey; and in-depth interviews of security subject matter experts. Data collected were analyzed quantitatively and qualitatively.

The study yielded mixed results, suggesting that a person's generation is not a significant factor in their understanding of NTK. Instead, individual characteristics, organizational culture, level of clearance, and training level on NTK seemed to have a greater effect on a person's understanding of NTK.

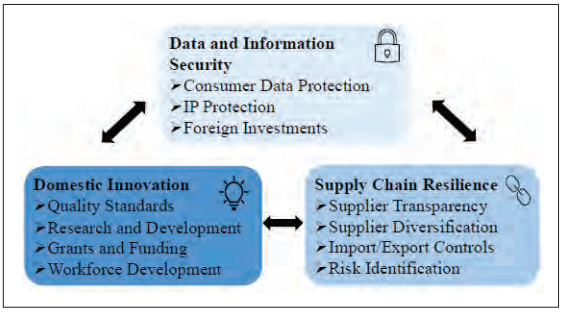
>> TEAM NY: Navigating the Regulatory Landscape: Impact on Biotechnology

GOVERNMENT TOPIC CHAMPION: Lauren Quattrochi (OUSDRE-STPP-MTA), A. Cody Youngbull (OUSDRE-STPP-MTA)
FACULTY MENTOR: Michelle Bensi
RISC INTERNS:

- Harrison Hill
- Sydney Mason

PROJECT ABSTRACT

Team New York was tasked with mapping and cataloging the regulatory landscape of the domestic bioeconomy and highlighting existing regulatory and policy strengths and weaknesses. By analyzing GAPS In the regulatory and policy landscape, Team NY identified opportunities to mitigate the effects of dependence on foreign biotechnology entities from the perspectives of domestic innovation, supply chain resilience, and data and information security. The purpose of identifying the strengths and weaknesses of the current landscape was to assess the ability of the U.S. to enhance resilience in biotechnology supply chains within the regulatory environment. The project goals were to determine the key existing regulation, policies, executive orders, and agency initiatives that may impact biotechnology supply chains, particularly from the perspective of the three identified themes of analysis. Further, we were tasked with conducting a case study analysis and assessing existing regulatory tools to mitigate foreign involvement in the biotechnology supply chain as well as establish improved resilience and redundancy in domestic supply chains to reduce the impact of system shocks.



Themes of Analysis

We approached this project by first collating regulatory, policy, and legislative measures from agencies or entities that influence this landscape and producing a matrix detailing key agency responsibilities and existing initiatives. These tools were sorted into domestic innovation, supply chain resilience, and data and information security. Next, we applied this framework to determine opportunities to mitigate their involvement in the U.S. bioeconomy and build redundancies in their place. Lastly, Team NY applied the lessons learned from the case study to a broader analysis discussing gaps in the existing regulatory and policy landscape and highlighting opportunities to improve the U.S. position in the specified project objective areas of supply chain resilience, domestic innovation, and data and information security.

>> TEAM PA: AI/ML to Support Defense Security Policy

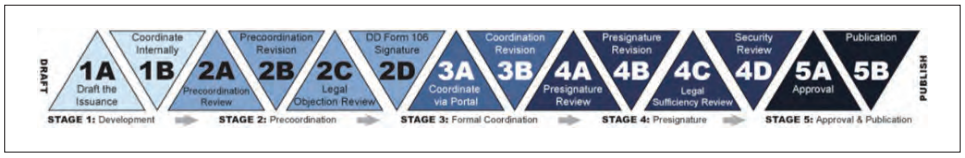
GOVERNMENT TOPIC CHAMPION: Amanda McGlone (OUSDIS-CLS)
FACULTY MENTOR: Allison Reilly
RISC INTERNS:

- Isabella Battish
- Preethi Pai

PROJECT ABSTRACT

The Department of Defense policy process timeline establishes the expected length of time to develop and issue new or revised policy (i.e., DoD Issuances) to be approximately 6-10 months. Despite this expectation, most DoD Issuances take substantially longer, sometimes multiple years, to complete. The process is encumbered by inefficiencies and consumes much of DoD policy analysts' time, preventing them from addressing other high priority tasks. The lengthy process also discourages policy change until required.

This project identifies areas in the policy process that are slow, why they are slow, and where AI and ML can be harnessed to expedite the process. The project takes a mixed methods approach of interviews and surveys with DoD policy analysts to unpack hurdles in the process and gather data on the issues in the process. Finally, we provide recommendations that could be explored further to expedite the policy adoption process.



Steps in the DoD Issuance Process

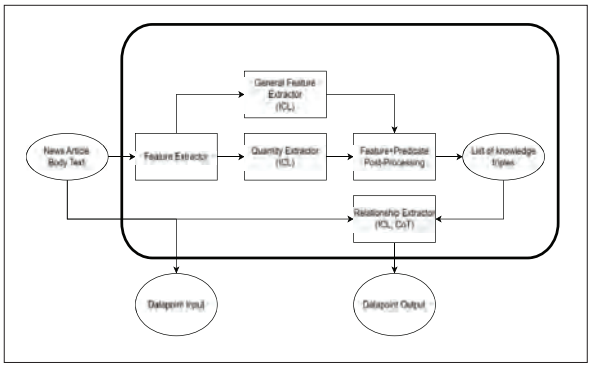
>> TEAM SD: Reducing Erroneous ML Observations Through Topological Reasoning

CHAMPION: Michael Lenihan (NGA)
FACULTY MENTOR: Paulo Shakarian (Arizona State University)
RISC INTERN:

- **Edward Wang (Johns Hopkins University)**

PROJECT ABSTRACT

With over 5,000 ports and 50,000 vessels sailing the ocean each day, it is increasingly important to have accurate models ensuring Safety of Navigation (SoN) and detecting and predicting illicit maritime events. As a result, the National Geospatial-Intelligence Agency is sponsoring a project to utilize free, publicly available data and knowledge graphs to develop systems that can detect infrastructure changes at ports. This information will be combined with satellite imagery and vision models to reduce the error and enhance the accuracy of information presented to analysts.



Feature Extraction Pipeline

An important aspect of this system is the task of knowledge extraction, taking unstructured textual data scraped from news articles, identifying important phrases containing information about port infrastructure, and outputting it in a structured RDF triple format. To do so, the NGA is using a FLAN-T5 model pre-trained on a synthetic dataset to extract knowledge into triples. However, using the synthetic dataset poses several issues that may impact the performance of the knowledge extractor. Since the dataset is synthetic and not from actual articles on port infrastructure, the performance of the finetuned model may suffer as the training dataset is not representative of the articles it will see. As a result, we are implementing an automated dataset generator using GPT-4. Taking advantage of the powerful language abilities of GPT-4, various prompting techniques, and postprocessing, we can build system that can generate datasets from real news articles. This allows us to create a higher quality and representative dataset that is also scalable to produce large datasets, resulting in better performance of offline finetuned LLMs required for security purposes.

This approach led to a precision of 0.75 and recall of 0.77 on the validation data set. When manually evaluated on unseen data, we calculated a precision of 0.76. Overall, our approach to dataset generation is promising with consistent performance on validation and unseen data.

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