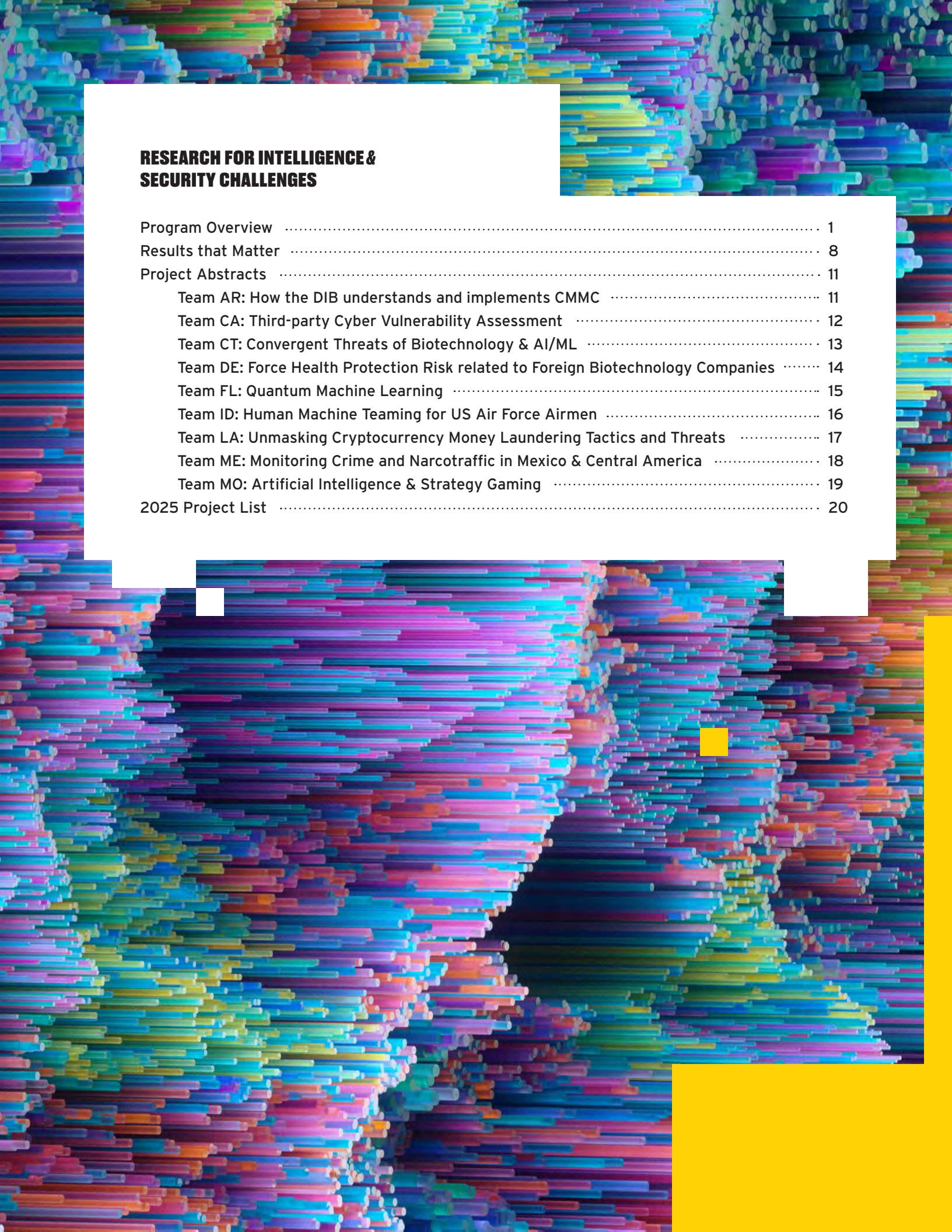
RISC

RESEARCH FOR INTELLIGENCE & SECURITY CHALLENGES

SUMMER INNOVATION SPRINTS

2025 PROGRAM REPORT



RESEARCH FOR INTELLIGENCE & SECURITY CHALLENGES

Building Tomorrow's Solutions and Cleared Workforce, Today

The Research for Intelligence & Security Challenges (RISC) program serves dual roles. RISC is a world class innovation sandbox to facilitate quick-turn applied research for mission-critical intelligence and security problems. It is also a premier pipeline for identifying, training, and launching the next generation of cleared technical talent for national security.

Run by University of Maryland's Applied Research Laboratory for Intelligence and Security (ARLIS), RISC recruits top-tier undergraduate and graduate students from across the country to tackle real problems for real mission sponsors work.

America faces a critical shortfall in cleared STEM and behavioral science talent. RISC closes this gap by:

- Delivering mission-relevant research with actionable impact
- Building and clearing a multidisciplinary talent pipeline aligned to defense and intelligence needs and drawn from a cross-section of communities nationwide
- Strengthening relationships between the U.S. Defense Intelligence and Security Enterprise and universities nationwide
- Cultivating early exposure to sponsor missions, agency partners, and classified career tracks

In 2025, 689 applicants were received from over 100 universities nationwide. The 88 students placed onto one of the 35 innovation sprint teams brought expertise in disciplines including:

- Aerospace Engineering
- Applied Mathematics
- Artificial Intelligence
- Biology
- Business Administration
- Chemical Engineering
- Cognitive Science
- Computational Linguistics
- Computer Engineering
- Computer Science
- Cyber Security Engineering
- Data Processing
- Data Science
- Electrical & Electronic Engineering
- Geography
- Industrial and Systems Engineering
- Information Science
- Information Systems
- Intelligence and Security Studies
- International Relations
- Linguistics
- Mass Communication
- Mechanical Engineering
- Philosophy
- Physics
- Political Science
- Psychology
- Public Administration
- Secure Embedded Systems
- Security and Risk Analysis

35

INNOVATION SPRINTS

Real Problems, Real Impact

Each summer, RISC students engage in sponsored research across ARLIS's core mission areas: open-source intelligence; information warfare; command, control, intelligence, surveillance & reconnaissance; human performance & readiness augmentation; acquisition & industrial security; and counterintelligence for strategic competition.

- AI/LLM development
- Competitive and impact analysis
- Data aggregation
- Gap analysis
- Geospatial analysis
- Hardware testing
- Linguistic analysis
- Policy analysis
- Program testing and evaluation
- Research roadmap development
- Software development
- Vulnerability assessment

A selection of detailed innovation sprint abstracts is included in this report to highlight the diversity and operational relevance of RISC research.

How It Works

Schedule

10-week virtual program with weekly touchpoints, mentor meetings, and sponsor engagement

Team

2-4 students per team, selected from top national universities through a competitive process

Mission

Mission-scoped challenges defined by government sponsors and supported with real data

Capstone

Final in-person capstone, where RISCers brief senior stakeholders and discuss outcomes with peers and government leaders in College Park, MD

Many RISC teams continue their work past the summer. In 2025, 30 of 88 RISCers extended their work with ARLIS into the fall semester, providing continued value to sponsors and strengthening the talent pipeline.

48

FACULTY MENTORS

Mentorship That Scales

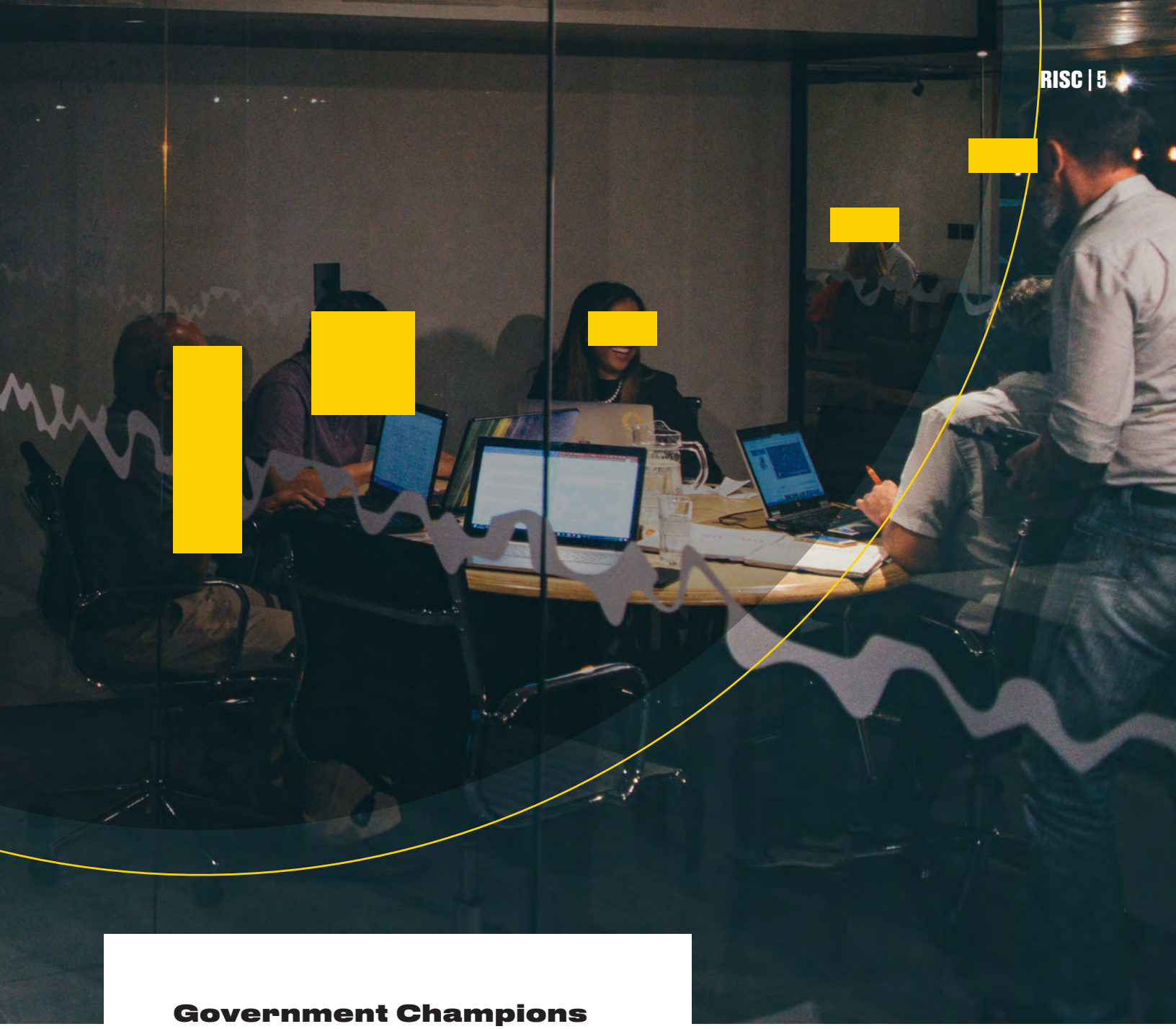
Every innovation sprint is supported by a pair of dedicated mentors:

- Faculty experts who translate complex sponsor problems into scoped projects that can be meaningfully addressed within 10 weeks
- Government champions who request the work and provide context, feedback, and mission alignment

In 2025, 48 faculty mentors supported 35 projects, including faculty from the broader INSURE research consortium and minority-serving institutions like Howard University and Morgan State.

This year's mentors came from a range of disciplines, including:

- Business
- Civil & Environmental Engineering
- Computer Science
- Cyber Security
- Data Science
- Electrical & Computer Engineering
- Geoinformation
- Human Computer Interaction
- Imaging Science
- Physics
- Policy
- Political Science
- Psychology
- Quantum Computing
- Remote Sensing
- Security Studies
- Software Engineering
- Systems Engineering
- Technology Test and Evaluation



Government Champions Drive Mission Relevance

RISC doesn't just simulate government problems - it generates usable solutions. In 2025, government champions from 18 organizations across the Defense Intelligence and Security Enterprise partnered with ARLIS to sponsor RISC research teams.

These champions:

- Provide real-world problem statements
- Supply relevant data or constraints
- Engage regularly with teams to guide outcomes
- Help assess deliverables for operational use

Their direct involvement ensures that every RISC innovation sprint is grounded in real national security mission requirement, not hypotheticals.

Exposure to the Mission, Not Just the Work

Throughout the program, students engage directly with experts from the defense and intelligence communities through ARLIS-led "Lunch & Learn" sessions, covering mission-critical topics such as:

- Roles and Responsibilities of the Intelligence Community
- Navigating the Shifting Federal Landscape
- Cognitive Biases in Security & Intelligence Decision-making
- Bridging Policy and Innovation Gaps
- Private vs. Public Sector Careers
- Cyber Operations
- Presenting Analysis to Decisionmakers

These sessions provide student researchers with further mission context, career insights, and direct access to senior voices in the field.

Delivering Impact

RISC projects don't stay on hard drives. They produce:

- **Usable deliverables:** Codebases, policy briefs, dashboards, simulations, risk models, and more
- **Operational outcomes:** Many teams brief senior leaders and contribute to ongoing program development
- **A cleared future workforce:** ARLIS helps students navigate the clearance process during and after the program

The end-of-summer RISC Research Showcase offers students the chance to present to government, academic, and industry leaders, strengthening their communication skills and visibility of their work.


RISC

Results that Matter

ROI for Intelligence and Security

427
STUDENTS SINCE 2020

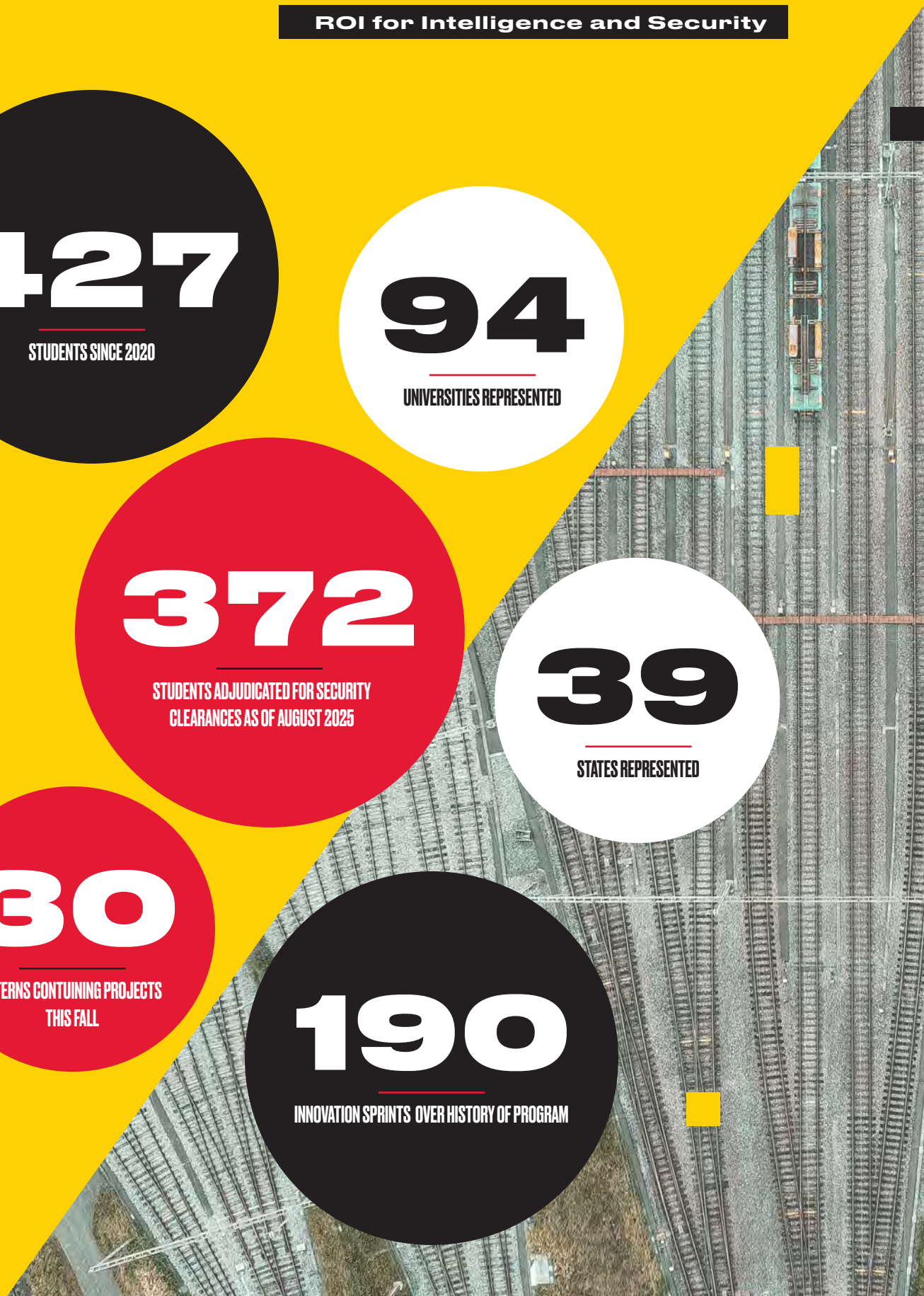
94
UNIVERSITIES REPRESENTED

372
STUDENTS ADJUDICATED FOR SECURITY CLEARANCES AS OF AUGUST 2025

39
STATES REPRESENTED

30
INTERNS CONTUINING PROJECTS THIS FALL

190
INNOVATION SPRINTS OVER HISTORY OF PROGRAM



A RISC Success Story: Declassification

The RISC innovation sprint platform not only produces quick-turn value for government stakeholders, but in some cases have grown from small student project to high-visibility, multimillion-dollar research programs.

In 2021, one of that year's 15 innovation sprint teams was asked to look at declassification across the DoD. Current declassification processes force reviewers to sift through mountains of paper records, an approach that leads to inefficiency, burnout, and high turnover among declassification personnel. That RISC work would lay the foundation for a multi-year effort to make classification and declassification more consistent, efficient, and transparent across the government.

The 2021 team analyzed existing workflows in detail, creating systems engineering diagrams to capture the complexity of the process. They conducted extensive interviews with specialists to understand their day-to-day challenges and opportunities for improvement. This human-centered approach guided the technical innovations that followed, both in year-round ARLIS R&D and additional rounds of RISC sprints.

The Office of the Under Secretary of Defense for Intelligence & Security (OUSD I&S) asked ARLIS to continue the work to reimagine the system from the ground up. RISC stayed central to innovation and development.

RISC 2022 sprint teams tested new technologies and developed a framework to consolidate and align more than 1,700 disparate declassification and security classification guidelines across agencies. 2023 and 2024 teams leveraged AI and machine learning to develop tools to automate repetitive tasks, improve search capabilities, and surface relevant information more quickly, all while keeping humans in the decision-making loop. 2025's Team KS continued the tradition.

This work has since attracted national attention. The Public Interest Declassification Board, a presidential advisory body created by Congress in 2000, praised ARLIS's efforts in letters to the U.S. President and Congress, citing the project as a model for applying digital tools to complex policy challenges. The letters also recommended reforms to Executive Order 13526 to help standardize classification systems nationwide.

Today, ARLIS and OUSD I&S are actively collaborating with government agencies to share best practices, test solutions, and build momentum for lasting reform. From RISC innovation sprint to major government investment, ARLIS is helping declassification processes evolve from a burdensome manual task into a streamlined, technology-enabled system, one designed for the realities of the 21st century.

RISC 2025 made me optimistic about the future of our defense and intelligence workforces. I'm so grateful for this opportunity - it was a privilege to learn from the examples you set at ARLIS."

The chance to work on projects directly supporting the defense and intelligence space and truly make an impact is incredible. and there's no other opportunity like the RISC program."

The excellent research delivered by the team demonstrates that even early-career analysts, examining open-source documents with rigor, can uncover trends and risks often overlooked in U.S. policy and national security discussions."

The students I worked with were diligent, creative, and deeply devoted to serving the broader national security mission of the US government. It was satisfying to watch their research and analytical skills develop considerably over the course of the internship."

PROJECT ABSTRACTS

Team AR

How the DIB understands and implements CMMC

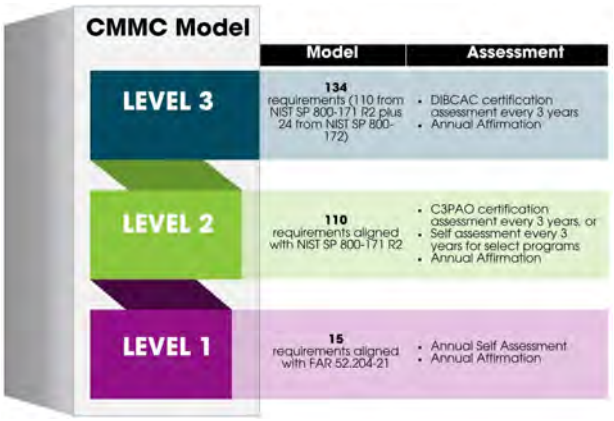
Government Champion
DTIC

Faculty Mentor
Natalie Scala

RISC Interns
Manasi Dixit | Emily Jones | Andrew McNeil

Abstract

The DoD and the IC will require the Defense Industrial Base (DIB) to hold Cybersecurity Maturity Model Certification (CMMC) to harden their systems that store, process, and transmit Controlled Unclassified Information (CUI). The project examines how clearly this requirement and the associated process is understood by the DIB, as well as whether CMMC achieves the DoD's desired outcomes and how it will continue to do so as the DoD implements the Zero Trust model. Through a survey and select subject matter expert (SME) interviews, the team contributes to the understanding of industry perspectives on CMMC and potential gaps or challenges in the process that they have experienced. The identification of gaps and challenges will be beneficial to future organizations seeking CMMC compliance, for the secure usage of FCI and controlled CUI in government contracts. Expected project outcomes include a position paper laying out the challenges companies face understanding and obtaining CMMC, an examination of the results of research into the quantitative risk reduction provided by the controls required to obtain different levels of CMMC, and an assessment of how CMMC will integrate with DoD Zero Trust architecture. This position paper will use the results of the survey, among other data collection methods, to determine what these challenges are.



Source: https://dodcio.defense.gov/CMMC/About/

Team CA

Third-party Cyber Vulnerability Assessment

Government Champion
Army Intelligence & Security Command

Faculty Mentor
Kelly Thomas

RISC Interns
Ella Antonishek | Rachel Wang

Abstract

Organizations depend on third-party vendors for advanced software tools and state-of-the-art commercial capabilities. However, this dependence introduces new vulnerabilities as these tools are external to the organization's systems and infrastructure and introduce uncertainty as to whether the software is regularly assessed, audited, updated, and patched. Determination of the security posture of a third-party vendor and its solutions become even more challenging as the US Government (USG) is not notified of significant changes or upgrades to vendor architecture or the vendor's auditing, vulnerability and risk assessment, and vulnerability and risk management processes, raising concerns about whether the software tool is truly secure. These third-party commercial tools often have additional third-party integrations, which only increase the attack surface and the number of potentially vulnerable system components that attackers can exploit to compromise the software. These upgrades and third-party integrations, in additional to poor cybersecurity practices and any other malicious or non-malicious actions that the vendors may take, intentional or not, leave not only third-party vendors but their customers vulnerable to cyber-attacks from adversaries and threat groups. The always-evolving threat landscape, the evolution of cybersecurity vulnerabilities, threats, and threat actors, and the emergence of new vulnerabilities in the digital age emphasize the important of proactive cybersecurity, continuous monitoring, and regular auditing and vulnerability assessments.

Team California (CA) will address this need by conducting a vulnerability assessment for the two Open-Source Intelligence (OSINT) tools which are utilized by the Army OSINT Office (AOO) for OSINT collection and research. The team will provide a comprehensive technical report documenting the vulnerability assessment process of these tools, results and key findings from the vulnerability assessment, the determined level of security, potential vulnerabilities, and technical and policy recommendations outlining security controls, training, and other actionable mitigation strategies that remediate the identified vulnerabilities and effectively manage third-party risk. The team's efforts will provide insights into the cyber risk posture of the evaluated tools and their vendors and ensure the continued security of USG systems and networks.

Team CT

Convergent Threats of Biotechnology & AI/ML

Government Champion
ONI

Faculty Mentor
Brian Weiss

RISC Interns
Kathleen Bostick | Trevor Casey

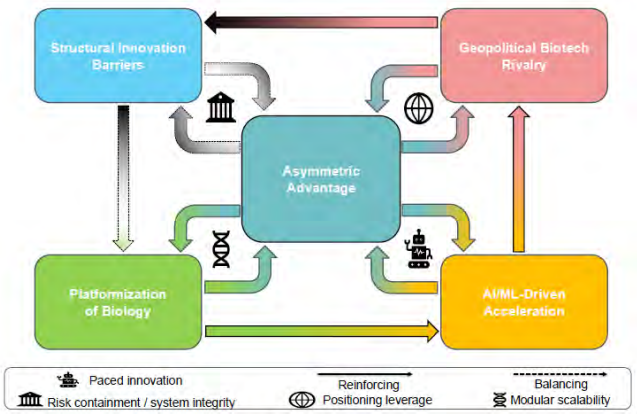
Abstract

To enhance national strategic advantage in biotechnology, it is crucial to have a foundational understanding of how artificial intelligence and machine learning (AI/ML) are impacting genetic engineering. These advanced technologies play a pivotal role in protecting the nation's security and preserving leadership in biotechnology. Genetic engineering's convergence with AI/ML presents a unique opportunity to assess innovations in genetic engineering, to articulate those elements that influence innovation, and to identify the key innovators.

This innovation sprint sought to explore how AI/ML are being applied to advance genetic engineering in precision medicine and human performance enhancement, and what factors most accelerate or inhibit biotechnological innovation. Project deliverables included an initial landscape mapping of current biotechnological research, the identification and quantification of factors that accelerate/decelerate biotechnological research, and a final report and presentation.

Through a structured literature review, more than 80 peer-reviewed sources contributed to mapping the current state of research and application and examine measurable indicators. These works help illuminate how biotechnology tools, including revolutionary gene editing technology, are enhancing the innovation ecosystem.

In parallel, the project lays the groundwork for a trend analysis of biotechnological progress from 2006 to the present, both in the United States and adversarial foreign entities. This effort enables future research to more rigorously examine longitudinal trends and model key variables that correlate with accelerated innovation in biotechnology research and development, as well as the barriers that slow it down. Findings are synthesized into a comprehensive final report that consolidates key takeaways and offers a forward-looking direction.



Team DE

Force Health Protection Risk related to Foreign Biotechnology Companies

Abstract

Given the significant, ongoing advances in synthetic biology, big data health analytics, and artificial intelligence and machine learning (AI/ML), there are growing concerns surrounding the popularity of direct-to-consumer (DTC) health products, especially those sold by foreign biotechnology ("biotech") companies to United States (U.S.) citizens. What happens to user data—who sees it, where it goes, how it gets stored—is not always apparent. Nonetheless, U.S. government and military personnel are largely permitted to use such products if they desire, potentially putting their privacy and security in jeopardy.

The aim of this project is to identify the risks associated with foreign biotech companies receiving health data from U.S. personnel, and the resulting implications for force health protection. To achieve this, Team DE assembled a case study digest that highlights 12 different incidences of data breaches in the biotech sector, exemplifying the types of vulnerabilities that foreign biotech companies may possess, and what can happen when these vulnerabilities are exploited.

Government Champion

I&S

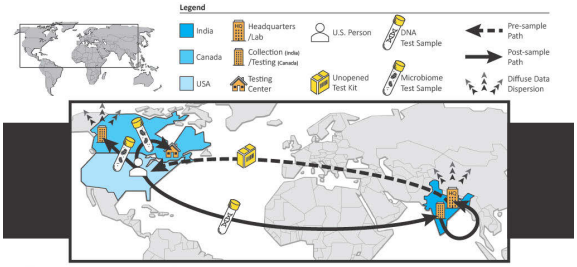
Faculty Mentor

Lauren Diaz

RISC Interns

Jillian Geib | Alanna Hennessey-Loyo

Figure 1. *Biological Sample Testing: End-to-End Test Kit Logistics*



Tables 1a-2b. *Risk Assessment of Biological Sample Testing*

Table 1a. *Risk Matrix with Overall Risk Score*

I \ P	Unlikely 1	Possible 2	Likely 3
Low 1	1	2	3
Medium 2	2	4	6
High 3	3	6	9

* **Risk Score** (R) equals the product of the **Impact** (I) and **Probability Scores** (P); *R=I*P*

Table 1b. *Key to Risk Score Interpretations*

Color Code	Risk Score	Interpretation
Major	6+	Use of company services carries **major risk**; U.S. personnel should avoid interacting with this company.
Moderate	3-4	Use of company services by U.S. personnel carries **moderate risk**. Caution advised.
Minor	1-2	Use of company services by U.S. personnel carries **minor risk**

Table 2a. *Risk Categories with Impact & Probability Scores*

Category	Impact Score	Probability Score
Company Location/ Operations	2	2
Handling of Data	2	1
Legal & Regulatory Compliance	1	1
Research Use	1	1

Table 2b. *Key to Impact & Probability Scores*

3	Impact: **High**
	Probability: **Likely**
2	Impact: **Medium**
	Probability: **Possible**
1	Impact: **Low**
	Probability: **Unlikely**

Additionally, Team DE utilized Open-Source Intelligence (OSINT) resources to gather extensive information on various foreign biotech companies operating in the U.S. This included details such as business transactions, supply chains, and privacy policies.

Ultimately, Team DE's research findings will better inform decision makers of the threats posed by foreign biotech companies, especially those with ties to adversarial nations, and provide the intelligence and security community with critical insights for protecting U.S. personnel and safeguarding national security.

Team FL

Quantum Machine Learning

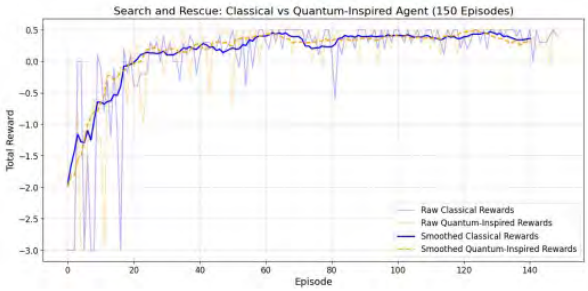
Government Champion
Air Force SAF/CDM

Faculty Mentor
Sonia Jallah, Sarah Miller

RISC Interns
Dranel Jiles | Aybars Kocoglu | Nico Mannarelli

Abstract

The development of quantum technologies has been motivated by the prospect of quantum advantage: significantly improved performance and utility of these technologies making them preferred over fully classical technologies in a practical setting. One area that seems promising in this regard is machine learning, which classically has many demonstrated effective use cases, such as in state-of-the-art artificial intelligence (AI). In particular, there is great interest in increasing model capabilities and learning efficiency using quantum resources and hardware (Zaman et al., 2025). As there is a major mismatch between the amount of data current Noisy Intermediate-Scale Quantum (NISQ) devices can process efficiently and the amount of data processing state-of-the-art machine learning models require, it has proven difficult to train and evaluate relevant quantum machine learning models. This bottleneck is one of data ingestion: how can classical data meaningfully and efficiently be converted and represented as quantum states for processing? Team FL investigates this bottleneck in the context of reinforcement learning and quantum transformer architectures to evaluate existing proposed solutions and propose potential new ones, seeking implications that allow them to better characterize quantum advantage.



Team ID

Human Machine Teaming for US Air Force Airmen

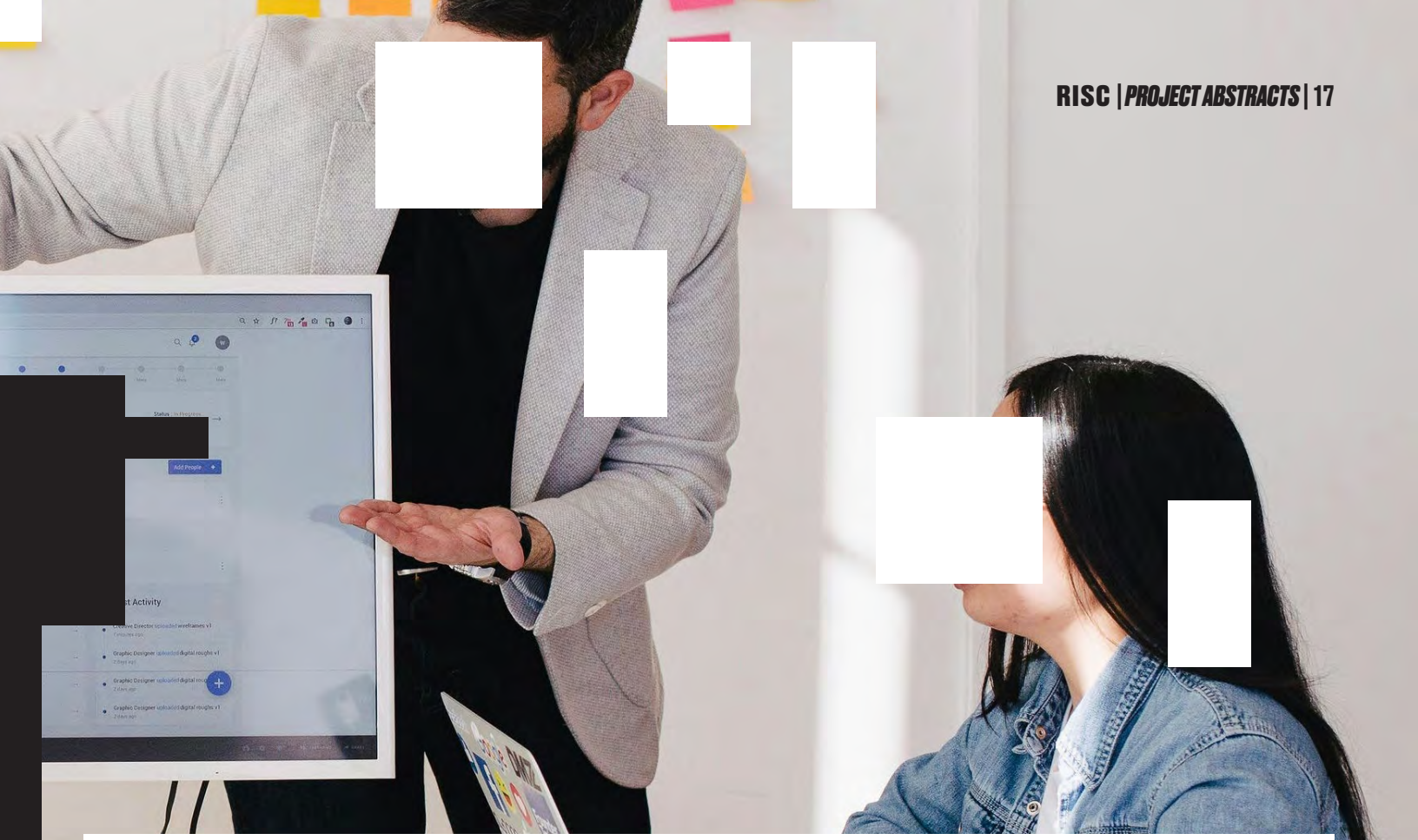
Government Champion
AF Integrated Capabilities Office

Faculty Mentor
Julie Marble, Melissa Carraway

RISC Interns
Aiden Hu | Christopher LeBlanc

Abstract

The project's purpose is to develop an initial understanding of how artificial intelligence (AI) and machine learning (ML) can be applied to human-machine teaming (HMT) tools to assist Airmen and Guardians in their daily roles. In service of that goal, this project seeks to: show the benefit of AI/ML HMT usage in the Air Force (AF) through the lens of improved human performance (HP), determine how AI/ML HMT can help make decision chains more resilient to human error, propose baseline AI-readiness requirements for Airmen and Guardians, and as a stretch goal, identify a specific problem within the air refueling (AR) planning domain, outline its solution requirements, and develop an AI/ML HMT prototype solution for it. To understand how AI/ML HMT and more specifically agentic AI systems can be implemented in the AF, the team approaches this project pragmatically through a case study on AR planning, generalizing as appropriate to the broader AF.



Team LA

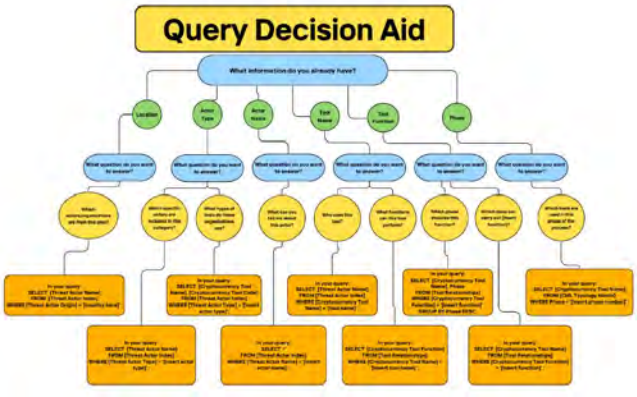
Unmasking Cryptocurrency Money Laundering Tactics and Threats

Government Champion
Air Force Intelligence Systems Support Office

Faculty Mentor
Paulo Shakarian

RISC Interns
Pilar Glaser | Cailyn MacLellan | Sydney Rothstein

It is increasingly clear that cryptocurrency has become a means for illicit actors to launder money; however, knowledge repositories and projections of relevant emerging technologies are limited. Previous research has documented the proportion of the cryptocurrency market that is touched by money laundering and common techniques used by illicit actors. Team LA developed a framework to enable systematic analysis of methods used to launder money through cryptocurrency channels and determine areas with a high risk of money laundering within the cryptocurrency cycle. Furthermore, the project identifies the illicit actors that utilize each of the available methods and the challenges these present. These developments are followed by the identification of emerging technologies that have the potential to be utilized to disrupt the money laundering cycle in the cryptocurrency environment,



particularly as they pertain to gaps in current law enforcement disruption methods. This work will allow for the identification of tools and the creation of an analytical product for identifying and mitigating money laundering threats in the cryptocurrency environment.

Team ME

Monitoring Crime and Narcotraffic in Mexico & Central America

Abstract

As recognized in the executive order designating many as Foreign Terrorist Organizations (FTOs), Mexico and Central American cartels and TCOs serve as primary facilitators for illicit trafficking into the United States, threatening the heath and security of the American public as well as our legitimate markets. Moreover, as Transnational Criminal Organizations (TCOs) have increasingly adopted the use of online platforms to coordinate their transnational criminal and drug-related activities, it has become increasingly difficult to combat their adverse impact, emphasizing a growing need for near-real-time-information. By exploiting foreign open-source data, Team ME aims to improve the Department of Defense's (DoD) ability to monitor and analyze crime and narcotrafficking in Mexico and Central America by aggregating relevant near-real-time Publicly Available Information (PAI) and Commercially Available Information (CAI) into an open-source repository. Not only will collecting open-source outlets that report on or for TCOs, including major cartels and gangs, facilitate a nuanced understanding of TCO activities, but it will also improve information sharing across federal, local, and state agencies due to the absence of classification requirements needed to access said sources. Overall, our compilation of open-source outlets (via media scraping, strategic searches, etc.) will support analysis and Southern Border operations by providing a streamlined method for collecting on crime and narcotrafficking topics.

Government Champion
Department of Defense

Faculty Mentor
Harrison Murray & Joe Kelly

RISC Interns
Sarah Curry | Riley Nelson | Saahil Rao

Team MO

Artificial Intelligence & Strategy Gaming

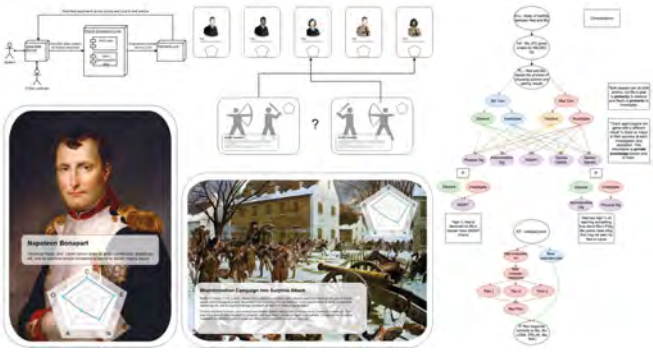
Government Champion
OUSD(I&S)

Faculty Mentor
Jason Spitaletta

RISC Interns
Peter Hartnett | Jacob Hardin-Bernhardt

Abstract

The concept of a computer system for playing a game has captivated the popular imagination in many ways, from the 18th century, when the chess-playing Mechanical Turk defeated players around the world, to the hit 1980s movie "WarGames", in which a computer attempts to execute a plan to win at Global Thermonuclear War. However, a common thread of these computer-played games is that they are most often perfect or near-perfect-information games, with clear rulesets and minimal ambiguity. Consider, by comparison, real situations of international conflict between state or nonstate actors—high levels of ambiguity about adversary intentions and, even with top-of-the-line SIGINT, ambiguity about adversary capabilities and resources. Recently, projects such as DARPA's SHADE and Meta's Cicero have focused on the capabilities of AI to handle the game Diplomacy—a situation of perfect tactical and capability information, but with ambiguity of intentions and trust among the players. This project seeks to introduce AI as a participant to a game environment with ambiguity and private information about capabilities as well as intentions. Specifically, the project explores scenarios of an Operational-level Deception process, in which both sides have perfect information about their own capabilities and intentions but limited or unreliable information about the adversary. Using COL Arnel David's thesis "Decision-making in the 21st Century: The Need for a Modern Day 'System of Expedients' to Win in War" as a basis for the project, Team MO will investigate the utility of AI systems in augmenting game environments of uncertainty or ambiguity for the edification of their players (David, 2023). Through this process, information will be gained about the potential of AI to integrate into the intelligence education process in a variety of ways, and its possible effects on future pedagogy.



2025 RISC Projects

TEAM AK: Threat Surface Analysis for Malicious Interaction Detection in Vision LMs | **Faculty Mentors:** Christopher Metzler (UMD), Ryan Thenhaus (ARLIS) | **Students:** Adam Baji (UMBC), Eric Guernsey (UMD), Anekah Kelley (Southern Methodist)

TEAM AL: Testing and Evaluation of Secure Facility and Vetting Technologies | **Faculty Mentors:** Katherine Forng (ARLIS), Moneer Helu (ARLIS) | **Students:** Xavier Francois (UMD), Faith Rodriguez (UMBC)

TEAM AR: How the DIB Understands and Implements CMMC | USG Champion: DTIC | **Faculty Mentors:** Natalie Scala (Towson) | **Students:** Manasi Dixit (UMD), Emily Jones (Howard), Andrew McNeill (Towson)

TEAM AZ: Assigning Value to Ambiguous System Security Risks | USG Champion: OUSD(R&E) | **Faculty Mentors:** Amir Ghaemi (ARLIS), Christopher Nissen (ARLIS) | **Students:** Ibrahima Diallo (GMU), Thomas Lapinig (Penn State)

TEAM CA: Third-party Cyber Vulnerability Assessment | USG Champion: Army INSCOM | **Faculty Mentors:** Kelly Thomas (ARLIS) | **Students:** Ella Antonishek (UMD), Rachel Wang (GMU)

TEAM CO: Delivering Uncompromised Capabilities | **Faculty Mentors:** Zachary Boyd (BYU) | **Students:** Jose Delgado (Texas A&M) , Zoe Klein (Michigan), Michael Venit (Loyola Maryland)

TEAM CT: Convergent Threats through the Intersection of Biotechnology & AI/ML | USG Champion: ONI | **Faculty Mentors:** Brian Weiss (ARLIS) | **Students:** Kathleen Bostick (Spelman), Trevor Casey (GWU)

TEAM DC: Policy Gaps and Lags in Emerging Technology and Innovation | USG Champion: OUSD(R&E) | **Faculty Mentors:** Timothy Leslie (GMU) | **Students:** Kristela Marie Avendano (UCSD), Meghan Hall (Georgetown), Ana Kisley (UNC)

TEAM DE: Force Health Protection Risk related to Foreign Biotechnology Companies | **Faculty Mentor:** Lauren Diaz (ARLIS) | **Students:** Jillian Geib (Rochester), Alanna Hennessey-Loyo (UMD)

TEAM FL: Quantum Machine Learning | **Faculty Mentors:** Sonia Jallah (ARLIS), Sarah Miller (ARLIS) | USG Champion: AF and DIA | **Students:** Dranel Jiles (Morgan State), Aybars Kocoglu (UMD), Nico Mannarelli (UMD)

TEAM GA: Quantum Encryption, Teleportation, and Secure Computing | USG Champion: SAF CDM | **Faculty Mentors:** Allison Casey (ARLIS), Gino Serpa (ARLIS), Darrell Teegarden (ARLIS) | **Students:** Asmita Brahme (UMD), Monic Moy (UCLA), Grace Yang (UMD)

TEAM HI: AI/ML Pipeline for Video Time-Space-Positioning Information | USG Champion: Army TECOM | **Faculty Mentors:** Alan McMillan (Wisconsin) | **Students:** Abhinav Kumar (Wisconsin), David Zikel (Wisconsin)

TEAM IA: AI Engineering Operations Research & Recommendations | USG Champion: ODNI | **Faculty Mentors:** Josh Poore (ARLIS), Alex Walter-Higgins (ARLIS) | **Students:** Joshua Cancio (GMU), Tyler Wilber (Georgetown), Theodore Wimberly (Carnegie Mellon), London Wolff (UN-Lincoln)

TEAM ID: Human Machine Teaming for US Air Force Airmen and Space Force Guardian | USG Champion: AF ICO | **Faculty Mentors:** Melissa Carraway (ARLIS), Julie Marble (ARLIS) | **Students:** Aiden Hu (UMD), Christopher LeBlanc (Northeastern)

TEAM IL: Counter AI Techniques Using Adversarial LLMs | **Faculty Mentors:** Henry Overos (ARLIS) | **Students:** Jonah Benjamin (UMD), Natalie Horton (UMD)

TEAM IN: LLM Agent Benchmarking Toolkit for Intelligence and Security | USG Champion: ODNI | **Faculty Mentors:** Evan Jones (ARLIS) | **Students:** Aline Jouaidi (UNT), Dhruvi Patel (UMD), James van Doorn (UMD)

TEAM KS: Exploring RAG and fine-tuning LLMs for information security and transparency | USG Champion: OUSD(I&S) | **Faculty Mentors:** Michael

2025 RISC Projects *(Continued)*

Brundage (ARLIS), Thomas Lu (ARLIS) **Students:** Kevin Lin (UMD)

TEAM KY: Curating an LLM Test Suite for Inferring Human Attributes and States | **Faculty Mentors:** Anton Rytting (ARLIS) | **Students:** William Lewis (Brandeis), Asher Moldwin (GMU)

TEAM LA: Unmasking Cryptocurrency Money Laundering Tactics and Threats | USG Champion: SAF CDM | **Faculty Mentors:** Paulo Shakarian (Syracuse) | **Students:** Pilar Glaser (UMD), Cailyn MacLellan (John Jay), Sydney Rothstein (Syracuse)

TEAM MA: Mexican Cartel Command and Control | USG Champion: DIA | **Faculty Mentors:** Eric McGlinchey (GMU) | **Students:** Isabelle Bree (UN-Lincoln), Jiahao-Jerry Lai (GWU)

TEAM MD: Chinese Foreign Investment Profiles | **Faculty Mentors:** Ed Gutierrez (ARLIS), Robert Schantz (ARLIS) | **Students:** Caroline Dinkel (GWU), Jonah Kocisko (UMiss)

TEAM ME: Monitoring Crime and Narcotraffic in Mexico & Central America | **Faculty Mentors:** Harrison Murray (ARLIS) | **Students:** Sarah Curry (Coastal Carolina), Riley Nelson (UMD), Saahil Rao (Georgetown)

TEAM MI: Unmanned Systems, Demography, and Mass | USG Champion: DIA | **Faculty Mentors:** Steve Sin (UMD) | **Students:** Tiffany Liu (UMD), Alexander Manes (Cal State Polytech), Sophia Tian (UPenn), Ella Voskamp (Slippery Rock)

TEAM MN: Understanding the Impact of China's Low Altitude Economy Strategy | USG Champion: FAA & FBI | **Faculty Mentors:** Allison Reilly (UMD) | **Students:** Zoe Bright (UNC), Erika Holdren (UMD)

TEAM MO: Artificial Intelligence & Strategy Gaming | USG Champion: OUSD(I&S) | **Faculty Mentors:** Jason Spitaletta (NIU) | **Students:** Jacob Hardin-Bernhardt (NYU), Peter Hartnett (Frostburg State)

TEAM MS: Will-to-Fight Framework Integration into a Kinetic Information Environment Simulation | USG Champion: Army DEVCOM | **Faculty Mentors:** Zachary Einolf (ARLIS) | **Students:** Avery Kops (UMD), Bennett Sellers (UMD)

TEAM NC: ICS Simulation Validation Exercise | **Faculty Mentors:** Ted Plettner (ARLIS) | **Students:** Dia Bonsu (UMD), Kavin Manivannan (UMBC), David Peabody (Texas Tech)

TEAM ND: Integrated Weapon Systems Data Management System | USG Champion: Army TECOM | **Faculty Mentors:** Jim Purtilo (UMD) | **Students:** Jenae Bothe (WashU), Andrew Podles (UMD), Adrian Strasser-King (UMD)

TEAM NE: Visual Media in APAC-Targeting Influence Efforts | USG Champion: AFRL | **Faculty Mentors:** Cody Buntain (UMD) | **Students:** Sravya Kotamraju (UT-Dallas), Gabriel Sankar (Georgia Tech)

TEAM NH: Threat Capabilities of Swarm Technology | USG Champion: ONI | **Faculty Mentors:** David Lovell (UMD) | **Students:** Zoe Bussewitz (Stony Brook), Jack Smoot (Gettysburg)

TEAM NJ: Electronic Signatures for Ship Classification | USG Champion: ONI | **Faculty Mentors:** Rajeev Barua (UMD) | **Students:** Cheyenne Bajani (GMU), Nithin Parepally (UMD)

TEAM NM: Defense Industrial Base Resiliency | **Faculty Mentors:** Tim Sprock (ARLIS) | **Students:** Donovan Decker (Texas A&M), Grant Heye (Texas A&M)

TEAM NV: Submarine Fleet Model Composability Analysis | USG Champion: Navy | **Faculty Mentors:** Joe Bradley, Ben Kassel, Dale Minich | **Students:** Leila Cornejo (UMD), Joanna Haley (Virginia Tech)

TEAM NY: GeoINT Methods for Supply Chain Anomaly Detection | USG Champion: NGA | **Faculty Mentors:** Michael Mann (UMD) | **Students:** Emma Loren (Georgetown), Sydney McDaniel (North Georgia), Gabriel Perry (BYU)

TEAM OH: Vulnerabilities in the Biomedical Supply Chain | USG Champion: OUSD(R&E) | **Faculty Mentors:** Shelby Bensi (UMD) | **Students:** Harrison Hill (UMD), Sydney Mason (GMU)

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

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

RISC 2025