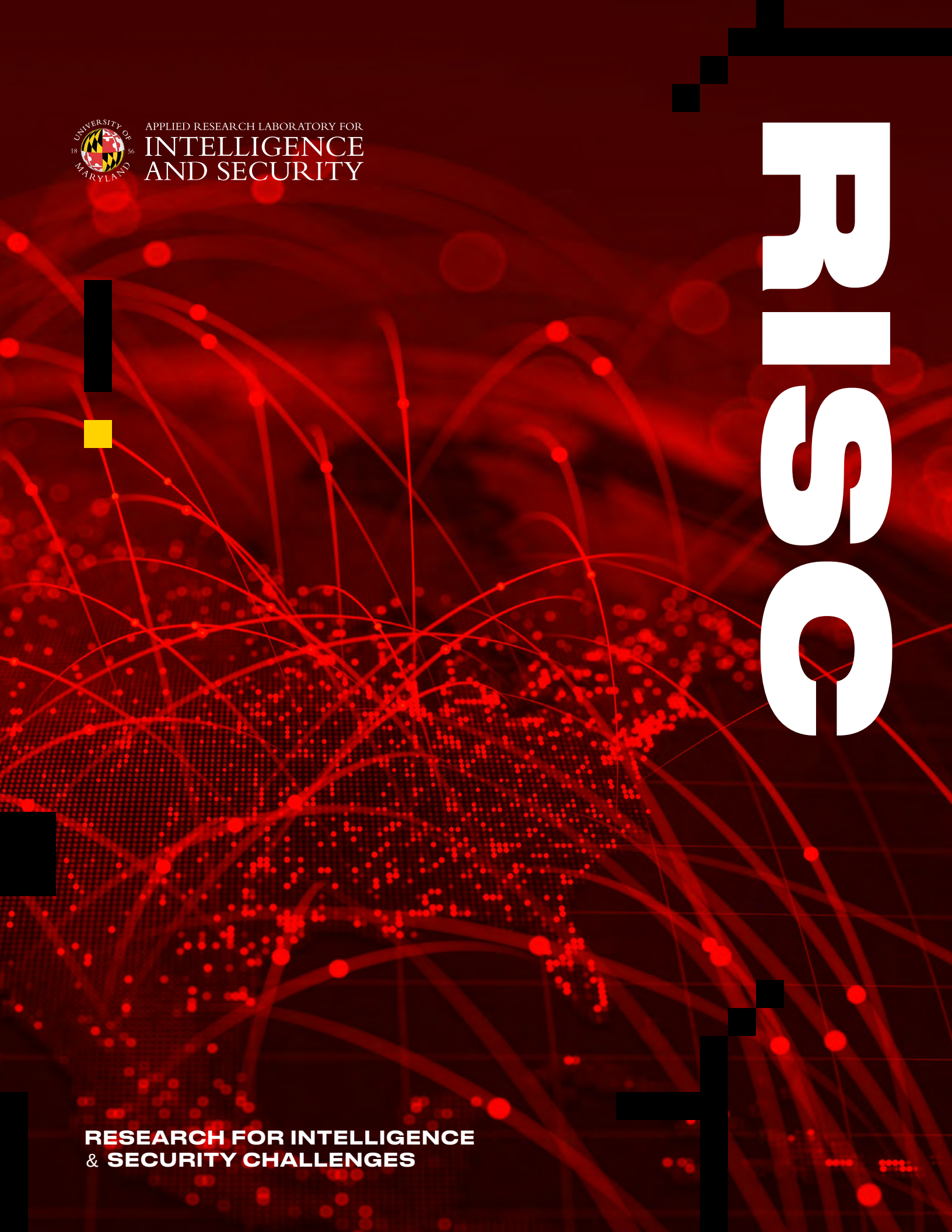

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY
RISC
RESEARCH FOR INTELLIGENCE
& SECURITY CHALLENGES

"From hacking away on VSCode to briefing at the Pentagon, I learned about the reality of integrating AI into government systems, present-day security challenges, and what it truly means to be a problem-solver...in only 10 weeks. "

RISC Student

TABLE OF CONTENTS

Program Overview **1**

Multidisciplinary Teams for a Multidomain Mission **3**

Program Outcomes **6**

Project Abstracts **10**

Special Access Program Personnel Security Questionnaire Database 10

Building an Enterprise Governance Framework for AARO in the Age of AI 11

Comparative Evaluation of AI Tools for Intelligence Analysis 12

Cybersecurity for Medical Autonomy in Casualty Care and Evacuation 13

Directed Energy Bioeffects Emerging Health Threats Keyword Extraction 14

Quantum x Biological Threats (QuBiT) 15

Modeling Quantum Clock Performance Outside the Lab 16

Ground Mission Survivability in a Contested Space Domain 17

Advancing Modeling and Simulation of Information Advantage 18

Security Implications of State-Owned Enterprise Mergers 19

2026 RISC Innovation Sprints and Team Affiliations **21**

PROGRAM OVERVIEW

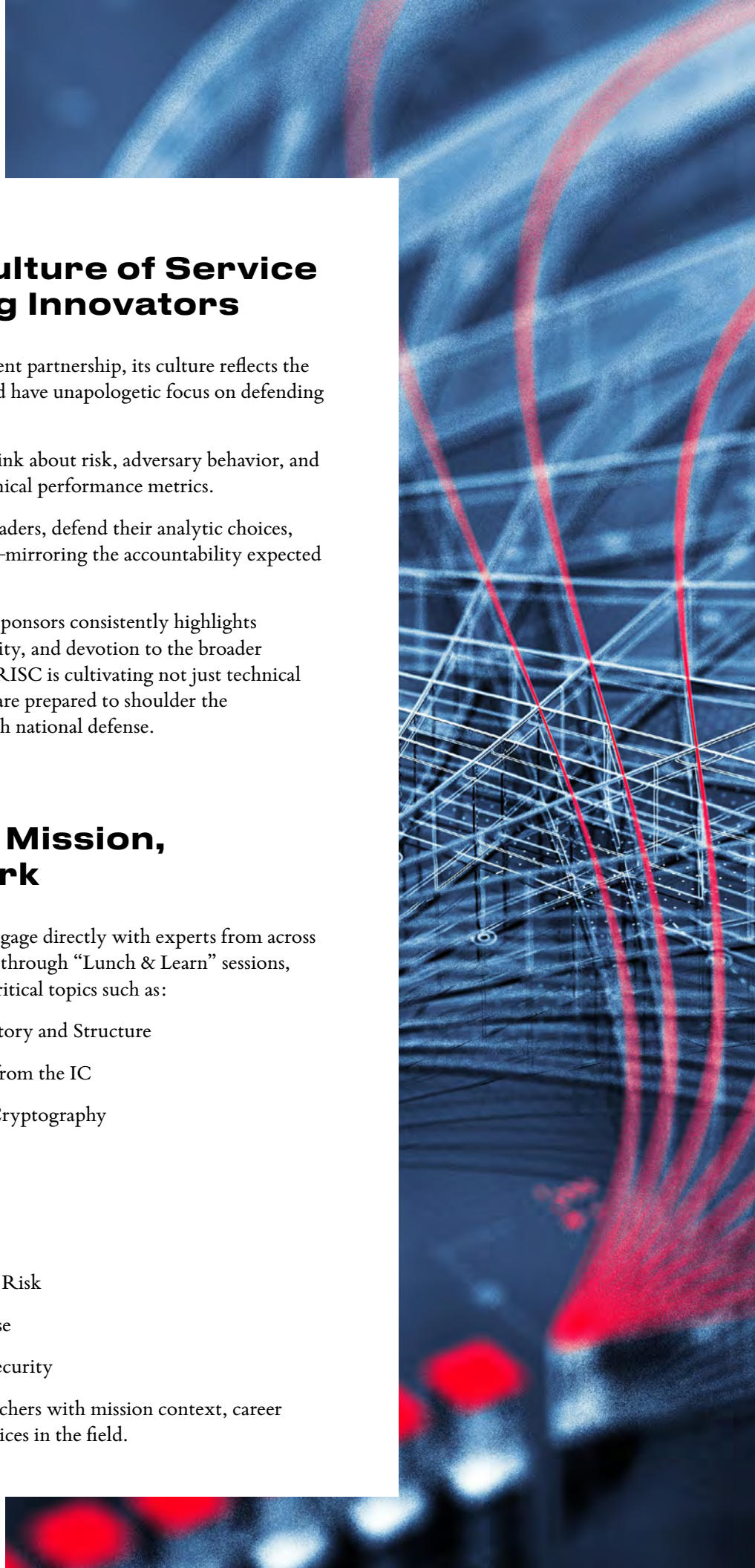
An Innovation Sandbox Developing Tomorrow's Cleared Workforce

The 2026 National Defense Strategy (NDS) is clear: defending Americans' security, freedom, and prosperity in a more dangerous world requires not only better capabilities, but also a deep bench of people who can think clearly, move quickly, and act pragmatically. The NDS directs the Department of War (DoW) to prioritize "missions that matter most for Americans' security, freedom, and prosperity," to supercharge the U.S. defense industrial base through creativity and ingenuity—especially in the area of artificial intelligence and other advanced technologies.

The DoW can only remain the nation's "sword and shield" if it has a workforce that understands the mission, can master rapidly evolving technologies, and is ready—cleared and committed—to serve.

RISC 2026 Innovation Sprint was designed to develop the skills and mindsets the nation needs:

- **Immersing students in real-world operational problems, not simulations.** Every RISC project starts from a government-generated problem statement tied to a concrete mission need—e.g., cyber resilience, interoperability, critical infrastructure, force health protection, or other challenges. Researchers learn to frame their work the way DoW and IC professionals must: in terms of threats, operational constraints, and tradeoffs, not abstract research questions.
- **Building cross-disciplinary operators for complex missions.** The 2026 NDS emphasizes integrating capabilities across domains and organizations. RISC mirrors this by forming teams that blend e.g., information science, engineering, social science, and regional expertise. Students learn to communicate across disciplines, work with ambiguous, imperfect data, and design solutions that are technically sound and operationally relevant.
- **Cultivating analytic rigor and a realistic mindset.** Through faculty and sponsor mentorship, students are pushed to be "clear-eyed" about evidence, gaps, and uncertainty—echoing the NDS's call to move "out with utopian idealism; in with hardnosed realism." They practice red-teaming their own assumptions, recognizing cognitive biases, and presenting tradeoffs candidly to decisionmakers.



Reinforcing a Culture of Service and Empowering Innovators

While RISC is an academic-government partnership, its culture reflects the NDS's call to empower innovators and have unapologetic focus on defending Americans' interests:

- Students are challenged to think about risk, adversary behavior, and consequences—not just technical performance metrics.
- Teams learn to brief senior leaders, defend their analytic choices, and accept critical feedback—mirroring the accountability expected inside DoW and the IC.
- Feedback from mentors and sponsors consistently highlights researchers' diligence, creativity, and devotion to the broader mission, demonstrating that RISC is cultivating not just technical talent but professionals who are prepared to shoulder the responsibilities that come with national defense.

Exposure to the Mission, Not Just the Work

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

- Intelligence Community History and Structure
- Cybersecurity: Perspectives from the IC
- Quantum Networking and Cryptography
- Open-Source Intelligence
- Human-Machine Teaming
- Information Warfare
- Operational Security/Insider Risk
- Biotechnology and Biodefense
- STEM Careers in National Security

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

MULTIDISCIPLINARY TEAMS FOR A MULTIDOMAIN MISSION

In Summer 2026, the RISC portfolio comprised 46 innovation sprints tackling a wide range of national security challenges, including artificial intelligence, cybersecurity, critical infrastructure protection, supply-chain resilience, force health protection, quantum technologies, and operational readiness.

Each sprint was scoped with a government sponsor and faculty mentor and executed in ten weeks. Teams moved rapidly from problem framing to usable products. Project outcomes included analytical frameworks, technical prototypes, decision-support tools, and policy recommendations that help sponsors understand emerging threats, harden critical systems, and make more informed strategic choices.

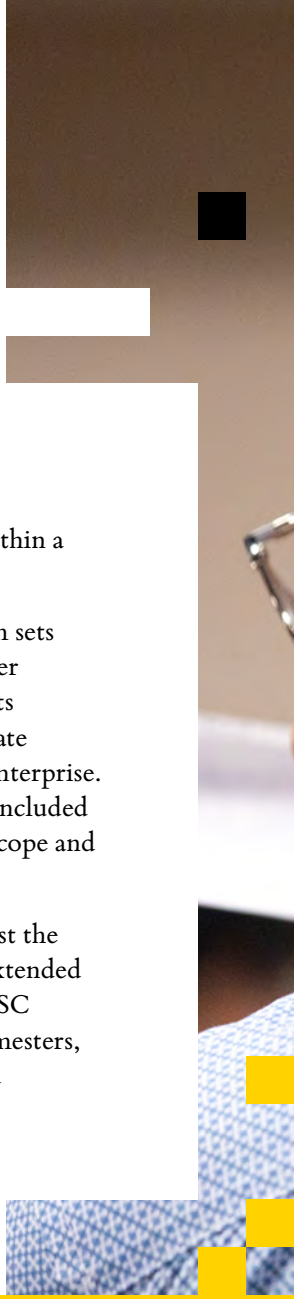
The multi-domain character of these problems demanded multidisciplinary teams. Projects combined methods such as advanced data analytics, systems modeling, red-teaming, vulnerability assessment, and policy analysis to illuminate both technical issues and their implications for warfighter readiness, industrial-base resilience, and strategic decision-making. Teams were formed around sponsor problem statements rather than academic departments, ensuring that each sprint brought together complementary skills rather than a single disciplinary view.

A National Talent Pool

To support this model, the 2026 RISC cohort drew from a wide span of academic backgrounds. 107 student researchers were selected from more than 800 applications across 45 states, reflecting both the competitiveness and geographic reach of the program.

Student researchers came from:

- Engineering (aerospace, mechanical, electrical, embedded systems)
- Computer and Information Sciences (computer science, computer engineering, information systems, data science, applied mathematics)
- Cyber and Security Engineering (cybersecurity, security and risk analysis)
- AI and Language Technologies (artificial intelligence, computational linguistics)
- Natural and Physical Sciences (biochemistry, biophysics, natural resources management, medicine)
- Social and Behavioral Sciences (psychology, cognitive science, economics, geography)
- Policy and Security Studies (political science, international relations, intelligence studies)
- Language and Humanities (linguistics, philosophy)



Teams Built Around Complex Problems

By cutting across a broad range of disciplines, teams were able to connect technology, operations, policy, and human behavior in ways no single field could achieve alone. Within individual sprints, engineers and data scientists worked alongside policy, regional, and social science students. A project developing measures of efficacy of AI in intelligence analysis leveraged backgrounds in political science, data science, psychology, and finance. Biochemists and psychologists reviewed the risks quantum technologies could pose to biodefense.

Students learned to translate across disciplinary languages, integrate diverse evidence streams, and align technical work with operational and policy needs. They absorbed complex mission context quickly and delivered outputs that sponsors could integrate into ongoing efforts, all within a ten-week window.

By pairing demanding, real-world problem sets with multidisciplinary teams of early-career researchers, RISC's 2026 innovation sprints showed how quickly new talent can generate usable solutions for the national security enterprise. A selection of detailed project abstracts is included on page 10 in this report to highlight the scope and operational relevance of RISC research.

Many RISC teams continue their work past the summer. In 2025, nearly 40% of interns extended their work with ARLIS (or began new RISC seedling efforts) into the fall and spring semesters, providing continued value to sponsors and strengthening the talent pipeline.

Mentorship That Scales

Every RISC innovation sprint is supported by a pair of dedicated mentors: a government champion to context, feedback, and mission alignment; and a technical faculty mentor to translate complex sponsor problems into tractable research projects and support project and student research oversight through the duration of the program.

In 2026, 49 faculty mentors supported 46 projects. While most RISC mentors were fulltime ARLIS researchers with security clearances, RISC also recruited faculty from the University of Maryland and partner universities including members of the ARLIS-led Intelligence and Security University Research Enterprise (INSURE) academic consortium.

> "[**Our RISC faculty mentor**] **has been an effective partner in facilitating communication, helping the students navigate a complex mission area and ensuring engagements remain focused, relevant, and value-added.**"
>
> *Government Champion*



Government Champions Drive Mission Relevance

RISC 2026 projects were requested and sponsored by 19 offices across the Defense Intelligence and Security Enterprise, including the Offices of the Under Secretary of War for Intelligence & Security and for Research & Engineering, the Army, Navy, Air Force, technology test and evaluation organizations, and intelligence agencies such as the Defense Intelligence Agency (DIA) and the National Security Agency (NSA). These sponsoring organizations spanned functional and regional offices, from policy to analytic tradecraft teams, acquisition specialists, and threat systems management.

Government innovation sprint representatives from these organizations—also known as "topic champions"—play a central role in the success of RISC sprints. They are responsible for proposing the project topics and in many cases resourcing the RISC student teams. Champions work closely with faculty mentors to scope broad problems into use cases or priority sub questions with the potential for meaningful initial findings over the course of a ten-week sprint. Champions help ground each project in the applied mission of their office, meeting with student researchers early in the summer to introduce the office or agency, explain its mission, and describe how the project fits into ongoing efforts.

Throughout the sprint, topic champions provide feedback on key deliverables and give students context on why the work matters, including potential career paths within the national security enterprise. For the final classified capstone, these government leads offer additional mission context. Champions participate in the RISC Research Showcase, where teams present their findings to a cross-section of stakeholders and demonstrate how the summer's work can be carried forward by their sponsoring organizations.

PROGRAM OUTCOMES

Results That Matter

RISC projects don't only stay on hard drives. Project outcomes included analytical frameworks, technical prototypes, decision-support tools, and policy recommendations that help sponsors understand emerging threats, harden critical systems, and make more informed strategic choices.

These innovation sprints produce:

- Usable deliverables: Codebases, policy briefs, dashboards, simulations, risk models, and more.
- Operational outcomes: Actionable findings briefed to senior leaders; shaping ongoing program development.
- Pathways to clearance: ARLIS helps students navigate the clearance process , enabling access to mission context and new career trajectories.

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



> **"RISC has confirmed that the defense and intelligence space is where I want to be, and it also expanded my perspective of how all disciplines contribute to our national security."**
>
> *RISC Alumna*



Clear ROI for the National Security Enterprise

Since its inception in 2020, ARLIS trained 530 RISC student researchers supporting more than 275 Innovation Sprints, with 490 of those students adjudicated for clearances. The RISC program expands the Defense Intelligence and Security Enterprise (DISE) talent pipeline by delivering mission-ready analysts who are steeped in real-world intelligence problems. Instead of replacing student training programs within the Combat Support Agencies (CSAs), RISC amplifies their impact by providing additional, DISE-wide training capacity and producing graduates who can deliver value to CSA missions Day One. Unique among internships supporting the intelligence and security communities, RISC offers:

- **National outreach with location flexibility.** RISC accepted students from 118 colleges and universities in 40 states, reflecting program prioritization on drawing from top talent nationwide and not only in the National Capital Region. Many talented students across the nation lack the exposure, professional networks, and understanding that their skills and knowledge can translate into national security careers. RISC promotes opportunities to work in the DISE to students who otherwise might not have known about these career options or would have difficulty taking advantage due to relocation requirements. By engaging these students, ARLIS provides opportunities for the future workforce to better reflect the nation as a whole.
- **Team focus.** RISC student researchers work in teams of other student researchers, with different technical backgrounds, on problems scoped to generate useable outcomes after only ten weeks. This rare opportunity for junior researchers to have real ownership of a project with direct applications builds confidence and enthusiasm for the work. RISC is differentiated from other research programs where most student interns, if they are fortunate enough to work on real problems, either work alone or contribute to a larger long-term effort for which they will never see the results.
- **Real problems and impact.** The program is an investment in the future of the national security workforce, but it also provides direct, immediate return for participating offices and agencies. RISC student researchers have supported more than 275 innovation sprints for the community and contributed thousands of hours of research, analysis, and technical expertise to hard, pressing issues within the intelligence and security enterprise. The students become active participants in the work, and in turn the sponsors gain access to talented students from a variety of academic backgrounds who bring new ideas and perspectives framing emerging best practices.

How RISC Shapes Careers: Alumni Profiles

ARLIS considers the training of the future workforce for the defense intelligence and security enterprise (DISE) to be one of its highest value outcomes. RISC program leadership engaged two interns from the RISC 2025 cadre to ask how their RISC experience helped prepare them for careers supporting the DISE mission.

Peter Hartnett

Summer 2025
Academic Year 2025 – 2026

Employer: Aerospace and defense company



For Peter Hartnett, RISC turned abstract academic interests into a concrete career path. He joined RISC in Summer 2025 and stayed on through the 2025–2026 academic year, supporting the Artificial Intelligence & Strategy Gaming innovation sprint. Soon after completing his RISC work, Peter was hired by an aerospace and defense company as an enterprise database architect—an opportunity he credits directly to his experience with ARLIS and the RISC program.

During his sprint, Peter discovered that he could build a career around what he genuinely enjoys: reading, learning, and solving complex problems. He recalls realizing that he was "being paid to read science journal articles, write about the contents, and propose solutions" as the moment he understood this could be his life's work, not just a summer internship. Working alongside professionals "focused on making a difference and keeping the nation safe," and presenting his team's work to Pentagon leadership, showed him that RISC projects "serve a real purpose" well beyond a typical class assignment.

Technically, RISC allowed Peter to move from theory to practice. He put algorithmic optimization into real AI-focused software, shifting from "maybe this will work" to "wow, that works—how cool is that?" In the process, he developed the patience, persistence, and steady determination required to see complex projects through from concept to completion—skills he still relies on in industry.

Equally important, RISC gave Peter exposure to the national security mission and the opportunity to attain security-clearance eligibility. That combination of hands-on technical experience and demonstrated commitment to the mission "really helped land my current position," he notes. Today, as he continues his career in defense industry, Peter points back to RISC as the moment when his interests in problem-solving and national security crystallized into a clear professional trajectory, with both the technical foundation and sense of purpose to sustain it.



Zoe Klein

Summer 2025
Academic Year 2025 – 2026

Employer: Applied Research Laboratory for Intelligence and Security



For Zoe Klein, RISC transformed national security from a distant, almost secretive career field into a place she could see herself—and ultimately did—belong. She joined RISC in Summer 2025, supporting the innovation sprint "Delivering Uncompromised Capabilities for Defense Acquisitions," then continued the effort through the academic year. Shortly afterward, she joined ARLIS full time, where she now analyzes how emerging technologies affect national security. By the end of the academic-year extension, she had "fallen more and more in love with ARLIS culture—the people, the work, and the mission"—and knew that a career supporting the national security mission was the right fit.

Before RISC, Zoe assumed that breaking into the intelligence community required being "recruited into the fold by someone wearing dark sunglasses and an earpiece." The program changed that perception. RISC showed her that she could, in her words, "recruit yourself to work in the intelligence and security enterprise" by developing her skills, doing high-quality work, and advocating for herself. What once felt like a closed world became an accessible, concrete career path.

The program also reshaped how Zoe approaches information and analysis. RISC taught her to read and understand complex material more quickly and comprehensively and—crucially—to apply what she learned to real problems rather than treating it as theory. Those habits now underpin her day-to-day work assessing emerging technologies for their national security implications.

With some distance from the experience, Zoe particularly values what RISC taught her about teamwork and responsibility. She notes that the level of responsibility entrusted to RISC researchers is "unique for students at our level" and mirrors the stakes of the workplace. Learning to "turn strangers into coworkers and coworkers into friends" while delivering for a real sponsor gave her a practical model for how effective teams operate in a mission-driven environment. Today, as a full-time analyst at ARLIS, she draws daily on the skills and confidence she built during RISC, in a career where she now helps shape how the United States understands and responds to emerging technology.



SELECT PROGRAM ABSTRACTS

Brief overviews of ten of 46 sprints from Summer 2026 - each with a unique state callsign - are highlighted. These efforts were selected both to share findings with the community and to demonstrate breadth of mission and topics and the variety of outcomes generated by RISC innovation sprints.

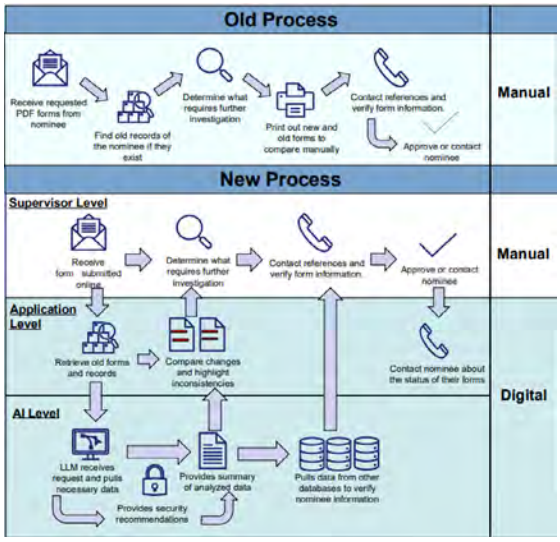
Project AR

Special Access Program Personnel Security Questionnaire Database

Government Champion: Office of the Under Secretary of War for Intelligence & Security (OUSW(I&S))

Carried out by student researchers from the University of Maryland and with mentorship from UMD faculty

The SAPCO enterprise requires anyone with a security clearance to complete forms disclosing their international relations or behavior issues to keep critical information safe. These forms are PDFs completed by the individual and mailed or emailed to the government who reviews the forms and updates the records manually. This project replaces the paper-based collection method with an intuitive, efficient, and secure database, paired with a web interface that enables users to submit forms and SAPCO personnel to review and update records with just a few clicks. The team built a realistic prototype for real-world implementation that allows the sponsor to explore the possibilities of this website and tweak the design before injecting real data and co-functionality with existing systems. Finally, this environment is ideal for testing the "art of the possible" with respect to AI integration, allowing SAPCO members to speed up workflow, detect suspicious activity, and automatically flag irregularities that may need to be fixed or addressed.



Comparison of the current manual review process for Special Access Program questionnaires and the workflow implemented in the developed prototype.

> **In most internships, you'll be given busy work or a toy project that they really don't care what the outcome is. At RISC, I got the opportunity to work on a project that has a real impact and has real value within the intelligence community.**
>
> *RISC Student*

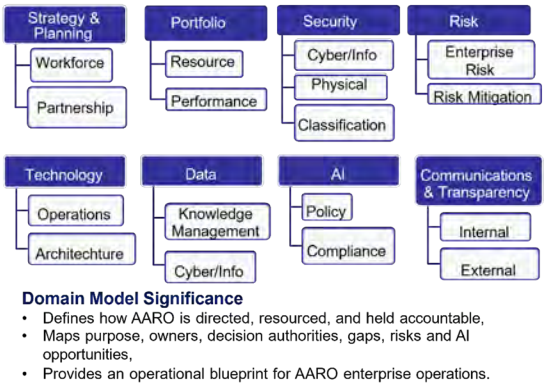


Project CT

Building an Enterprise Governance Framework for AARO in the Age of AI

Government Champion: OUSW(I&S) All-domain Anomaly Resolution Office

Carried out by student researchers from the University of South Carolina, University of Wisconsin, and Virginia Tech, with mentorship from University of Wisconsin faculty.



Core organizational governance domains and relevant subdomains.

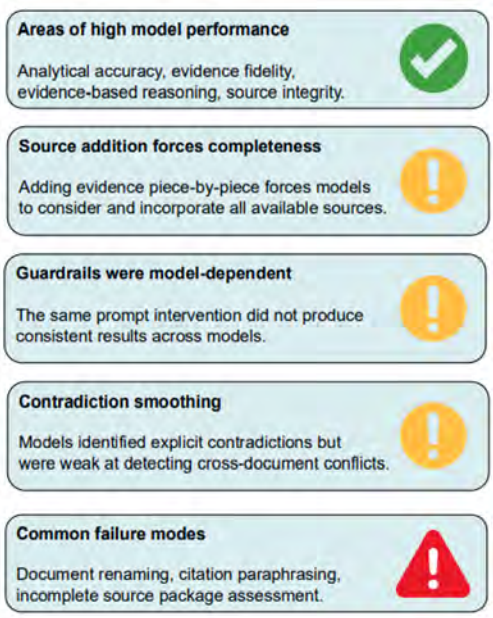
An established Enterprise Governance Framework can greatly help a department to create consistency that aids in decision-making structures, accountability mechanisms, organizational transparency, and performance management. As the All-domain Anomaly Resolution Office (AARO) continues to mature, the organization recognizes the need for consistent governance to align resources with mission priorities, improve decision quality, reduce organizational risk, and establish repeatable processes that scale as the organization grows. This project addressed the question – How can AARO establish an Enterprise Governance Framework that improves organizational effectiveness, accountability, transparency, and decision-making while leveraging Artificial Intelligence (AI) in a secure, responsible, and mission-focused manner?

In developing an Enterprise Governance Framework, the researchers explored methods for AI implementation across eight governance domains specific to the stakeholder, shown in the figure below with relevant subdomains: Strategy & Planning, Portfolio, Technology, Data, Artificial Intelligence, Security, Risk, and Communications & Transparency. The team developed recommendations for adopting AI to accelerate governance activities and guidance for introducing and implementing these capabilities responsibly across these domains. Further, this project examined real-world organizational challenges, evaluated emerging AI capabilities, developed executive-level recommendations, and presented findings to senior leadership.



Project DC

Comparative Evaluation of AI Tools for Intelligence Analysis



Qualitative card summary of Project DC best practice recommendations

Government Champion: Defense Intelligence Enterprise

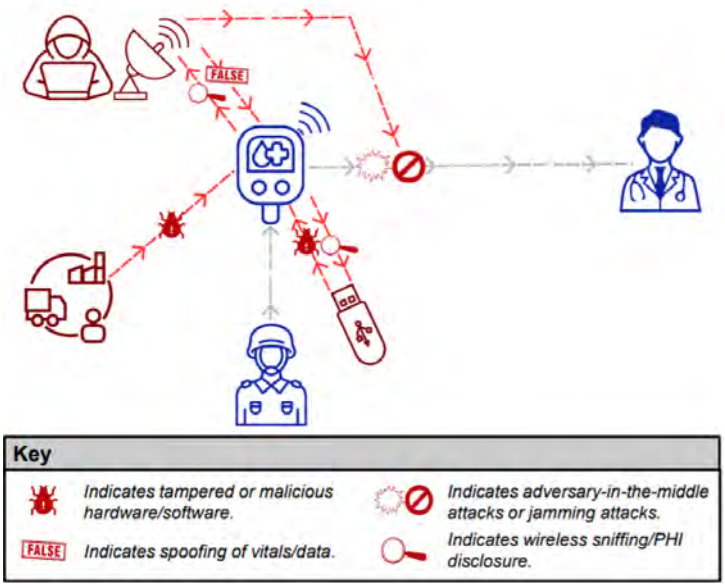
Carried out by student researchers from John Jay College, University of Wisconsin – Stout, and West Virginia University, with mentorship from UMD ARLIS researchers

AI tools are rapidly entering intelligence workflows. This project developed and applied a standardized benchmarking framework to evaluate AI tools across an evidence-grounded intelligence analytic workflow. The framework evaluated analytical accuracy, evidence fidelity, evidence traceability, evidence-based reasoning, completeness of analysis, and response to prompt variation. Using consistent tasks, source packages, prompt conditions, and scoring criteria, the project enabled objective, comparable assessment of tool performance. The result is a reusable benchmarking framework and a practical guide for identifying where AI tools enhance analysis, where they introduce risk, and how to integrate them effectively into intelligence operations.



Project IL

Cybersecurity for Medical Autonomy in Casualty Care and Evacuation



A vulnerability mapping for a wireless vital signs monitor, including supply chain, network, and physical attacks

Government Champion: Office of Naval Research

Carried out by student researchers from Southern Methodist University and University of North Georgia, with mentorship from UMD ARLIS researchers

Medical devices play a critical role in the assessment, treatment, and care of casualty cases in Naval operations, enabling field medics and the U.S. Navy hospitals to effectively treat injured warfighters. Newly developed autonomous and semi-autonomous devices create new treatment options for remote care and mechanized decision-making. These devices, however, may contain hidden vulnerabilities that leave them open to adversarial cybersecurity attacks, potentially exposing Protected Health Information (PHI) or serving as a stepping-stone for further network access. Similar attacks in the private sector—including the Stryker Corporation cyberattack, the Contec CMS8000 leak, and the WannaCry ransomware attack—demonstrate a strong motive for adversaries to attempt similar hijacks on devices used by the U.S. Navy.

This project assessed potential cybersecurity vulnerabilities in three devices commonly used by the U.S. Navy and in two operational scenarios. The first scenario evaluated the risk when used during treatment of a gunshot wound suffered on an island in the Pacific Ocean, and the second during treatment of myriad burn injuries suffered on a ship in the Pacific Ocean. The evaluation analyzed potential vulnerabilities caused by the usage of the three devices independently, in conjunction with a second device, all together, and in communication with the Navy Medicine Readiness and Training Command (NMRTC) San Diego.

This research provides the Office of Naval Research (ONR) with a comprehensive review of the cybersecurity threats to each device and begins to establish a framework of analysis that can be applied to other devices.



Project KY

Directed Energy Bioeffects Emerging Health Threats Keyword Extraction



Non-kinetic threats of importance to the Department of War include those in medical domains.

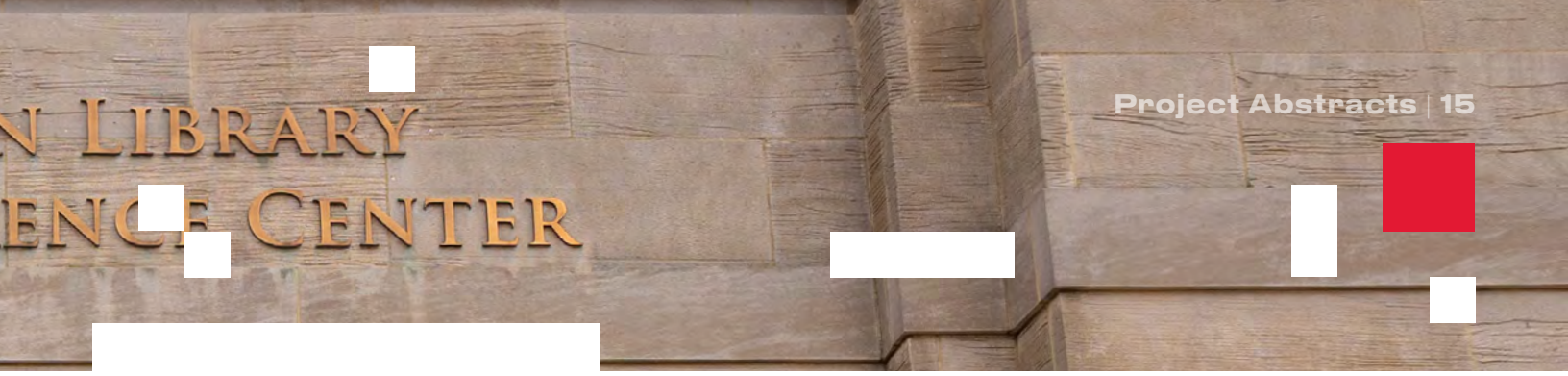
Government Champion: Office of the Undersecretary of War for Research and Engineering

Carried out by student researchers from Baptist University College of Osteopathic Medicine, University of North Georgia, and Georgetown, with mentorship from UMD ARLIS researchers

RISC 2026 Project KY supported an on-going ARLIS Directed Energy Bioeffects Emerging Health Threats (DEB) project sponsored by the Office of the Undersecretary of War for Research and Engineering (OUSW(R&E)). The primary RISC deliverable was a three-tiered keyword list from most general terminology (Tier 1) to most technical terminology and methods (Tier 3) across several advanced biological and neurological research domains. By incorporating these additional high-risk domains, DEB can mitigate bias that would limit a future DE health repository to only bioeffects and health threats related to DE.

To optimize the keyword list construction process in the future, a secondary goal of this project was to produce and compare six keyword extraction methodologies: manual, bibliometric (three approaches) and semi-automatic (two approaches). The manual method was the most extensive and found the greatest number of technical terminology when compared to the other methods by extracting words not just from author keywords and titles, but also from abstracts and introductions. Semi-automatic methods were limited by the PDF preprocessing step but should be explored and optimized further in the future as these methods are not limited to bibliometric meta data. Bibliometric methods were significantly hindered by analyzing only bibliometric data and not having access to the full text of an article; that said, they were the fastest and highest performing methods (roughly an hour and a half to employ, compared to the two-week timeframe required for manual extraction). No tested method outside of the manual method was successful at finding an extensive list of Tier 3 words. It is therefore necessary to further optimize the keyword extraction methods to be both efficient and high quality and explore the application of AI in keyword extraction. Subject matter expert curation after automated extraction remains a critical step in finalizing keywords and appropriate Tiers.

These keyword lists serve to supplement work already done previously for directed energy (DE) specifically, and they will be used by DEB in the future to design multidisciplinary search queries to populate a repository related to DE and emerging health threats.



Project MA

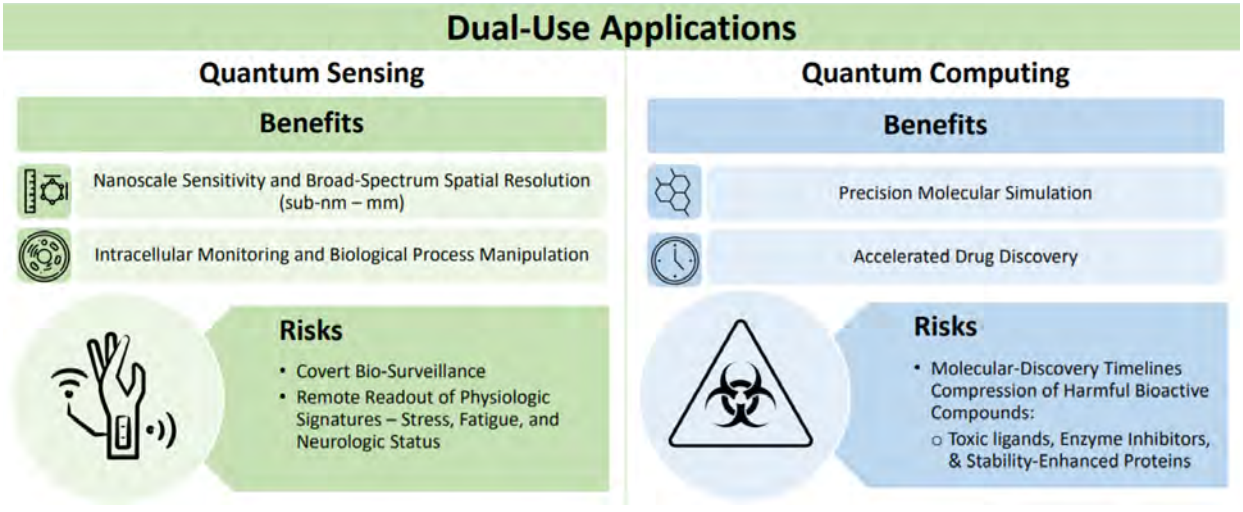
Quantum x Biological Threats (QuBiT)

Government Champions: Air Force Concepts, Development, and Management (SAF/CDM) and U.S. Army Nuclear and Counter-WMD Agency (USANCA)

Carried out by student researchers from University of Maryland, College Park and Georgetown University, with mentorship from UMD ARLIS researchers

The advent of quantum technologies, such as quantum computing and sensing, and their prospective advantages over classical counterparts have led to significant scientific and commercial interest in their applications to biological systems. Despite growing attention and investment in this field, documentation remains limited on key U.S. and foreign players operating in the "quantum x biology" domain, as well as the dual-use applications of these emerging technologies.

This project addresses that gap through a three-part approach: 1) identify key players advancing "quantum x biology" research, 2) map and categorize the core research and applications areas, 3) theorize potential dual-use applications with relevant risks to U.S. national security and intelligence. Key players were identified through open-source research, including IBM's collaboration with The Cleveland Clinic on quantum machine learning algorithms for drug development, the University of Chicago's work on quantum sensors based on molecular qubits, and the Japan Institute for Quantum Life Sciences' work on nitrogen vacancy nanodiamond sensing technology. Publication analyses conducted using Web of Science and tailored keyword parameters further highlighted the top three countries leading research output in quantum computing and sensing. While these technologies offer promising medical advancements, such as advanced precision medicine and accelerated drug discovery, continued research and monitoring are needed to evaluate the feasibility and timing of potential future risks as quantum technologies and their applications evolve.



Quantum technologies in biology offer transformative benefits for precision medicine and diagnostics while presenting potential dual-use risks, but continued research and monitoring are needed to evaluate the feasibility and timing of potential future risks as quantum technologies and their applications evolve.



Project ME

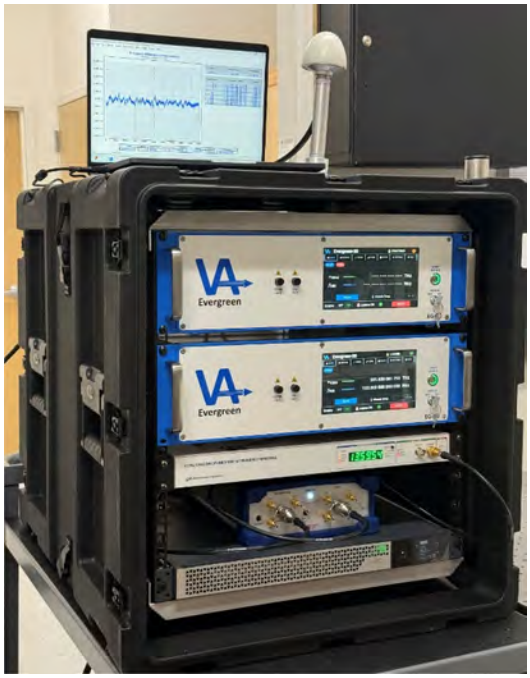
Modeling Quantum Clock Performance Outside the Lab

Government Champion: Secretary of the Air Force Office of Concepts, Development, and Management (SAF/CDM)

Carried out by student researchers from University of Maryland, College Park and University of North Georgia, with mentorship from UMD ARLIS researchers

Many think clocks are simply devices for keeping time, but in today's interconnected world, they serve as some of the core components for applications like GPS, astrophysics, and telecommunications. Current deployed precision timing systems rely on microwave atomic clocks, but a new generation of commercial optical atomic clocks may provide dramatic improvements.

This project evaluated these new timing devices and their performance to develop better and more efficient systems than the ones in current use. The team numerically simulated radar and very-long baseline interferometry (VLBI) applications of these clocks, two remote sensing applications of interest to the U.S. Air Force. Optical clocks measure time using atoms at higher frequencies with lasers, resulting in finer timing resolution compared to microwave clocks. Following recent commercial developments, new optical clocks combine high timing performance with deployable form factors, allowing them to be smaller, weigh less, and consume less power than leading commercial microwave clocks like hydrogen masers. Specifically, in comparison to hydrogen masers when used in VLBI, our findings show that optical clocks enable greater stability. This research shows how optical clocks push the boundaries of remote sensing capabilities, overall advancing the practical use of quantum technologies.



Two optical atomic clocks and measurement equipment mounted in a ruggedized case for field testing outside the ARLIS Quantum Clock Lab



Project MO

Ground Mission Survivability in a Contested Space Domain

Government Champion: U.S. Army Nuclear and Countering Weapons of Mass Destruction Agency

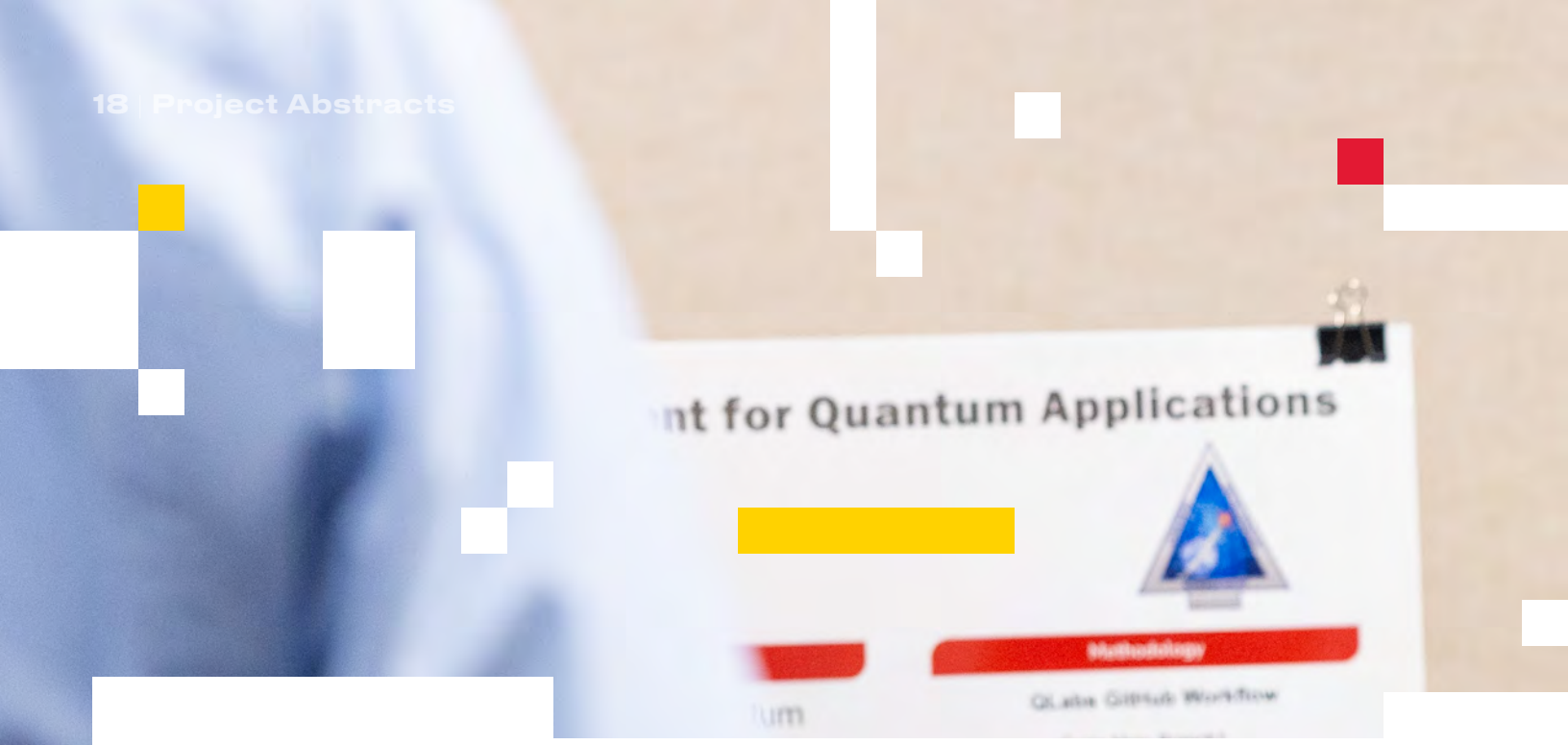
Carried out by student researchers from The George Washington University and Rochester Institute of Technology, with mentorship from UMD ARLIS researchers



System Survivability: Survivability = f (Susceptibility, Vulnerability), extended with Recognition & Recoverability. A Crown Jewel is any asset whose single-point loss causes total failure of ≥ 1 mission objective.

The U.S. Army conducts ground operations that increasingly depend on space-based position, navigation, and timing (PNT) and satellite communications (SATCOM) services—most of which the Army does not own but draws from U.S. Space Force systems. When an adversary denies or degrades those services through electronic warfare, the Army must understand how the resulting loss of PNT and SATCOM propagates into ground-mission failure.

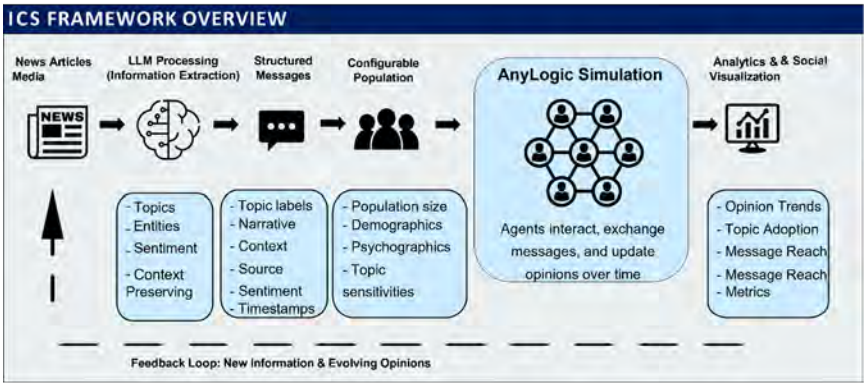
This research developed a repeatable methodology to assess that exposure. Six representative PNT and SATCOM systems the Army relies on were identified and assessed for their survivability—focusing on their susceptibility and vulnerability to jamming and spoofing—across two ground-mission threads: a battalion deployment and movement, and a Global Positioning System (GPS)-guided munitions strike. Applying a crown-jewel analysis to isolate mission-critical assets and a standardized survivability matrix to score them, the team determined which systems were least survivable yet most critical and prioritized them for mitigation. The result is a reusable, requirements-oriented process that exposes survivability gaps in Army ground systems and gives the United States Army Nuclear and Countering Weapons of Mass Destruction Agency (USANCA) a prioritized basis for protection and procurement decisions.



Project VA
Advancing Modeling and Simulation of Information Advantage

Government Champion: Office of the Under Secretary of War for Intelligence & Security (OUSW(I&S))

Carried out by student researchers from New York University and University of Maryland, College Park, with mentorship from UMD ARLIS researchers



A visual overview of the workflow leveraged by the ARLIS Information Competition Simulator (ICS) tool.

Information operations increasingly rely on understanding how information spreads through populations and influences beliefs, opinions, and behaviors. The ARLIS Information Competition Simulator (ICS) is an agent-based modeling (ABM) system designed to analyze these dynamics by simulating how individuals consume, exchange, and react to information.

This project investigated the feasibility of implementing ICS using an alternative ABM platform that included a configurable relational data model and new methods to represent information content. As a result, the team was able to develop a configurable relational data model that separates agent characteristics, variables, and reference data into reusable structures. The project also explored new methods for representing the information content by moving beyond simple sentiment-based packets towards richer, context-aware messages generated from media content using Large Language Models (LLMs).

The team developed a prototype implementation, evaluated its ability to support larger agent populations, and examined how structured information can be exchanged between agents through social networks and trust relationships. The results provide insight into the practicality of a more scalable and flexible architecture for information influence simulation and help guide future development of the ICS.

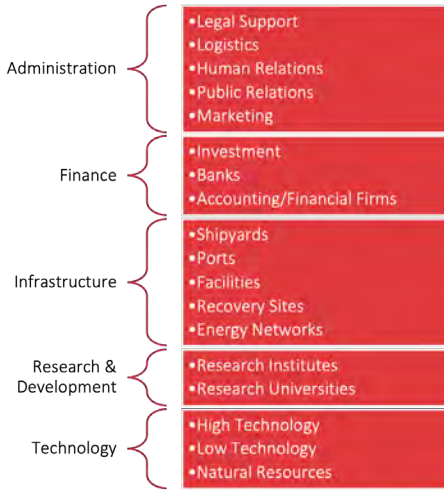




Project WI
Security Implications of State-Owned Enterprise Mergers

Government Champion: Office of Naval Intelligence

Carried out by student researchers from University of Texas at Austin and Johns Hopkins School of Advanced International Studies, with mentorship from UMD ARLIS researchers



Taxonomy of ship building company subsidiaries

In 2019, Beijing merged its two largest shipbuilding conglomerates creating the China State Shipbuilding Corporation (CSSC). In 2024 alone, this state-owned enterprise built more commercial ships than the entire U.S. shipbuilding industry since the end of World War II. CSSC's industrial capacity, combined with President Xi Jinping's "Military-Civil Fusion" (MCF, 军民融合) framework, enables the People's Liberation Army Navy (PLAN) fleet expansion and modernization, generating real security externalities for the U.S. military in the Pacific.

This innovation sprint mapped the People's Republic of China's (PRC) shipbuilding industry (SBI) supply chain by studying CSSC subsidiaries and analyzing the ecosystem of actors through link analysis. The researchers developed a taxonomy of shipbuilding companies, leveraging commercially available data to discover, collect, and place companies in the wider CSSC ecosystem.



"Through RISC and ARLIS, I've met fantastic mentors, worked on interesting projects, and been able to talk to people already in their careers to get insights on my own."

RISC Student





2026 RISC INNOVATION SPRINTS AND TEAM AFFILIATIONS

TEAM AL: AI/ML Tools to Enhance Installation Access Control | Mentor: Towson University faculty | Student researchers from George Washington University and Southern New Hampshire University

TEAM AR: Special Access Program Personal Security Questionnaire Database | Mentor: UMD faculty | Student researchers from University of Maryland

TEAM AZ: Humanitarian Notification System Assistance Tool | Mentor: UMD faculty | Student researchers from George Mason University and University of Maryland

TEAM CA: Automating Validation and Cataloging of OpenStreetMap Data | Mentor: George Mason faculty | Student researchers from George Washington University and University of Nebraska at Lincoln

TEAM CO: AI-Powered Search and Analysis for OUSW(I&S) Issuances| Mentors: ARLIS faculty | Student researchers from George Washington University, UMD, and University of Maryland Baltimore County

TEAM CT: Building an Enterprise Governance Framework for AARO in the Age of AI | Mentor: University of Wisconsin-Madison faculty | Student researchers from University of South Carolina, University of Wisconsin-Madison, and Virginia Tech

TEAM DC: Comparative Evaluation of AI Tools for Intelligence Analysis | Mentor: ARLIS faculty | Student researchers from John Jay College of Criminal Justice, West Virginia University, and University of Wisconsin-Stout Polytechnic

TEAM DE: Tactical AI for Next Generation Identity Intelligence | Mentors: UMD faculty | Student researchers from Georgetown University and George Washington University

TEAM GA: Dataset Attribution from Test Samples | Mentor: University of Missouri faculty | Student researchers from UMD and University of North Carolina at Charlotte

TEAM HI: Automating Object-Process Modeling for System Interoperability and Effectiveness Testing | Mentors: UMD faculty| Student researchers from UCLA and Howard

TEAM IA: Operational Constraints for Tactical Swarm Autonomy | Mentors: UMD ARLIS faculty | Student researchers from UMD

TEAM ID: Securing Intelligent Swarms | Mentor: Syracuse faculty | Student researchers from UMD and Brigham Young

TEAM IL: Medical Autonomy for Use in Casualty Care and Evacuation: Cybersecurity Considerations | Mentor: UMD ARLIS faculty | Student researchers from Southern Methodist University and University of North Georgia

TEAM IN: Neuromodulation to Augment Human Performance, Reduce Stress, and Mitigate Fatigue | Mentor: UMD ARLIS faculty | Student researchers from Syracuse and American University

TEAM KS: Biomicrorobots for Treatment and Prevention | Mentors: UMD ARLIS faculty | Student researchers from University of Michigan and George Mason

TEAM KY: Directed Energy Bioeffects Emerging Health Threats Keyword Extraction | Mentors: UMD ARLIS faculty | Student researchers from Baptist University College of Osteopathic Medicine, University of North Georgia, and Georgetown

2026 RISC Innovation Sprints and Team Affiliations Continued

TEAM LA: Developing a Security Classification Guide (SCG) Framework for the Biodefense Community | Mentor: UMD ARLIS faculty | Student researchers from UMD, Spelman College, and Syracuse

TEAM MA: Quantum x Biological Threats (QuBiT) | Mentors: UMD ARLIS faculty | Student researchers from UMD

TEAM MD: Mojo/GPU Code Development for Quantum Applications | Mentors: UMD ARLIS faculty | Student researchers from University of Maryland Baltimore County and UMD

TEAM ME: Modeling Quantum Clock Performance Outside the Lab | Mentors: UMD ARLIS faculty | Student researchers from UMD and University of North Georgia

TEAM MI: Bluetooth De obfuscation: Fingerprinting BTLE Devices | Mentor: Howard faculty | Student researchers from UMD and Morgan State University

TEAM MN: Redefining Mission-Critical Survivability Against Directed Energy Threats | Mentor: UMD faculty | Student researchers from UMD and Brigham Young

TEAM MO: Ground Mission Survivability in a Contested Space Domain | Mentor: UMD ARLIS faculty | Student researchers from George Washington University and Rochester Inst of Technology

TEAM MS: Assessing Agentic AI Risk | Mentor: UMD faculty | Student researchers from UMD, Rutgers, and Johns Hopkins

TEAM NC: Agentic AI & Cybersecurity: Mitigation Framework Design | Mentors: University of Wisconsin–Madison faculty | Student researchers from Purdue, UCLA, and University of Maryland Global Campus

TEAM ND: Survivability in the Age of Autonomy | Mentors: UMD ARLIS faculty | Student researchers from Gettysburg College and University of Arizona

TEAM NE: Joint Cyber Intelligence Tool Suite Refactor with GenAI | Mentor: UMD ARLIS faculty | Student researchers from UMD and University of South Carolina

TEAM NH: The Efficacy of AI Agents in Collecting Sensitive or Incriminating Information during Interviews | Mentor: UMD faculty | Student researchers from Arizona State and Rochester Inst of Technology

TEAM NJ: Strategic Messaging for Identity Intelligence Adoption | Mentor: UMD faculty | Student researchers from University of Nebraska-Lincoln and Eastern Kentucky University

TEAM NM: Training Data for Post Compromise/ Spill Scenarios | Mentor: UMD ARLIS faculty | Student researchers from University of Maryland Baltimore County and UMD

TEAM NV: SENTINEL: Secure Environment Website Risk Assessment Tool | Mentor: UMD faculty | Student researchers from West Virginia University and Smith College

TEAM NY: Complex System Decomposition for Criticality Analysis | Mentor: UMD faculty | Student researchers from University of Wisconsin-Madison and Brigham Young

"RISCers are some of the smartest and most productive students I have worked with in my career. My undergraduate team's productivity and innovation exceeded many graduate students and full-time professional engineers."

RISC Mentor

TEAM OH: Addressing Financial Concerns in Continuous Vetting: Best Practices, Gap Analysis, and Recommendations | Mentor: UMD faculty | Student researchers from Arizona State and Vanderbilt

TEAM OR: Rapid Content Collection Tool for High- and Low-Density Languages | Mentors: UMD ARLIS faculty | Student researchers from University of Washington and Rutgers

TEAM PA: LLMs and Multilingual Code Switching | Mentor: UMD ARLIS faculty | Student researchers from Iowa State, University of Vermont, and UMD

TEAM RI: Operations Security (OPSEC) for Science and Technology Acquisitions Projects and Programs | Mentor: UMD ARLIS faculty | Student researchers from University of Maryland

TEAM SD: Quantifying Digital Exposure for the U.S. Government Accountability Office: A Risk Assessment Framework for the DoW's Publicly Accessible and Unofficial Communications | Mentor: Rutgers faculty | Student researchers from Georgia Tech, Southern Methodist University, and George Mason

TEAM TN: Developing an OSINT Repository for Collection on Colombia | Mentor: University of South Carolina faculty | Student researchers from Coastal Carolina and George Washington University

TEAM TX: Enhanced Situational Awareness of Russian Activities in Developing Nations | Mentors: UMD ARLIS faculty | Student researchers from Emory and Georgetown

TEAM UT: Characterizing Information Security for Department of War Capabilities | Mentor: George Mason faculty | Student researchers from UMD and Brigham Young

TEAM VA: Advancing Modeling and Simulation of Information Advantage | Mentor: UMD ARLIS faculty | Student researchers from New York University and UMD

TEAM VT: AI-Enabled Detection of Adversarial Information Warfare Campaigns in the Southern Hemisphere | Mentor: UMD ARLIS faculty | Student researchers from UT Austin, UMD, and Davidson College

TEAM WA: Adversary Cyber Order of Battle | Mentors: UMD ARLIS faculty | Student researchers from University of Wyoming, University of North Georgia, and University of Massachusetts Amherst

TEAM WI: Security Implications of State-Owned Enterprise Mergers | Mentor: UMD ARLIS faculty | Student researchers from UT Austin and Johns Hopkins

TEAM WV: Feasibility Assessments for AI Data Centers | Mentor: University of Nebraska at Omaha faculty | Student researchers from UMD, Fordham University, The Institute of World Politics

TEAM WY: Scientometric Techniques for Identifying Technology Advancements, Innovations, and Breakthroughs | Mentor: UMD faculty | Student researchers from Cornell and University of Oklahoma


RISC