APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

RESEARCH FOR INTELLIGENCE AND SECURITY CHALLENGES

>> 2022 INTERNSHIP PROGRAM

PROGRAM REPORT / FALL 2022

RESEARCH FOR INTELLIGENCE AND SECURITY CHALLENGES

INTERNSHIP PROGRAM

RISC Program Report

Select Project Abstracts Summer 2022

RISC: CREATING AND NURTURING STUDENT TALENT

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

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

Leveraging Talent Nationally to Address Real-World Challenges

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

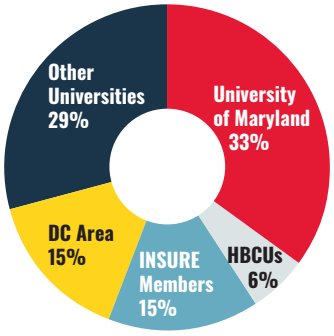
RISC targets students from various disciplines including science, technology, engineering, mathematics and social science fields. Many of the students come from the University of Maryland. However, most come from other institutions, including the ARLIS-led Intelligence & Security University Research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

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

GOALS

- Real projects for real end-users: Work on stuff that matters!
- Learn about national security careers and engage directly with members of security and intel communities
- Research exposure: open ended questions, experimentation, exploration, self-directed, etc.
- Help build the future technical workforce of the Intelligence Community and the Defense Security Enterprise
- Support talented students and important projects into academic year + initiate security clearances as appropriate

WHERE OUR INTERNS COME FROM



"I would have never touched on cybersecurity at this depth had it not been for the program. It has introduced me to a possible education and career path I would want to pursue."

–RISC INTERN TESTIMONIAL

"I think the program has made me very marketable to employers and has probably helped me land two job offers just by mentioning in interviews that I was participating in the program."

–RISC INTERN TESTIMONIAL

Disciplines of Interest

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

1. **Computer Science, Information Science & Engineering:** AI/ML algorithmic development, HCI, software engineering, systems engineering, media analysis and forensics, information systems design, geographic information systems, AI Assurance, Human 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 included **Measurement and evaluation of learning outcomes, environmental modeling and remote sensing, human factors, and regulatory public policy.**

INTERN DEMOGRAPHICS

- 103 interns from 37 institutions selected from 175 candidates (6x growth in two years)
- 64 undergraduates or recent grads (22 BA, 42 BS)
- 29 MA/MS students
- Nine PhD students,1 MD student
- Six returning interns from RISC 2021
- Seven interns from HBCU / MSI schools
- 55 from INSURE Consortium universities (36 from UMD)
- 48 from outside the National Capitol Region

In 2022, ARLIS received 175 applications from 54 universities and 103 students were selected from 37 universities.

The students selected for RISC 2022 brought backgrounds including:

- Anthropology
- Business
- Chemistry
- Communications
- Computer Science
- Criminology
- Cybersecurity
- Geographical Sciences
- Government and Politics
- Information Science
- Intelligence Analysis
- Languages and Linguistics (18 with significant foreign language expertise)
- (Applied) Mathematics
- Medicine
- Physics
- Psychology
- Public Affairs / Policy
- Security
- Sociology
- Statistics

TEAM MD: "Mapping Crop Types in Data-Sparse Regions"
- Elizabeth Dobbs, University of North Georgia
- Rishi Sinha, University of Illinois Urbana-Champaign
- Nicholas Shoemaker, University of Maryland Baltimore County

TEAM SD's final presentation, "Investigating Approaches to Modernize Classified Information Management"
- Samuel Mahowald, University of Wisconsin
- Jennifer Proctor, UMD

TEAM NC: "Improving Cyber Threat Disclosures"
- Christopher Lidard, Princeton University
- Edmund Kargbo, UMD
- Virgil Sermon, UMD

The class of 2022 supported 40 projects benefiting 14 defense and intelligence agencies. Topics included:

- Creating predictive analysis to identify critical and emerging technology companies susceptible to foreign investment.
- 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 40 intern projects are included in this report, representative of the wide range of problems tackled.

The RISC Experience

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

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

"RISC provided me with opportunities to expand my skillset, especially w/ machine learning and artificial intelligence. RISC also has pushed me to move more towards intelligence/national security research (hopefully through a continuation into the fall/spring)."

–RISC INTERN TESTIMONIAL

"I'm actively pursuing a defense career that hadn't even crossed my mind a year ago. Having applied research experience makes me actually competitive and qualified for those roles."

–RISC INTERN TESTIMONIAL

- Aethiopia Joseph-Salmon, Howard University

- Nathalie McGinn, George Mason University
- Yemlibike Fatkulin Haris, American Military University

- Krehl Kasayan, UMD
- Arin Zeng, UMD
- Kaleb Schmucki, UMD
- Jamie Cantwell, New York University

"I felt like the most rewarding aspect of ARLIS was the opportunity to interface with subject matter experts across various fields related to Defense and Intelligence. I will take away the connections I made with professors of practice, faculty research specialists, Lunch N Learn speakers and fellow colleagues. ARLIS RISC created and sustained a network of similarity motivated individuals with unique backgrounds, skillsets, and approaches to solving hard security challenges."

—RISC INTERN TESTIMONIAL

Given mutual interest between the sponsor and interns and available funding, RISC projects often continued into the academic year, sustaining sponsor connectivity beyond the original 10-week period. In 2022, 35 interns continued their work at ARLIS.

Connecting Interns to the Intelligence and Security Communities

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

Extending the lunch-and-learn model, 2022 RISC program staff facilitated small group discussions between four-to-eight interns and a current or former senior official from the defense or intelligence communities. Supplementing the large-group lunch-and-learns, the small group sessions enabled real multiparty discussion on topics like careers in counterintelligence, government-wide stakeholders working to countering malign influence, and how military cyber security work differs from elsewhere.

For the first time in 2022, ARLIS held a job fair, securing participation from government sponsors, FFRDCs, national labs and industry. The interns attended cross-sector information sessions, received guidance on searching for jobs, and participated in informational interviews.

Program Outcomes

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

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

Ultimately, the RISC program aims to attract new talent to the Defense Department, intelligence community, and larger security and intelligence enterprise by exposing top students to interesting work in support of a compelling mission. Though the program remains young, early data indicate a clear return on investment: of the 38 interns who participated in summer 2021, 14 were employed by the government, the defense industry or ARLIS as of October 2022.

"I didn't really know what I wanted to do before I joined RISC. Now I know I definitely want to work in the intelligence sector with the government. I had the chance to speak with some very skilled people and got some of their wonderful insight."

—RISC INTERN TESTIMONIAL

"I feel more prepared to brief/ present on information I researched after the weekly roundups and final capstone event. I still don't know where in the intelligence and defense community I would most like to work, but I feel I better understand what specific skills I can bring to a particular position in the future."

—RISC INTERN TESTIMONIAL

TEAM NY: "Measuring the Quality of Learning from Simulations"
- Lillian Stout, Princeton University
- Ethan Morrow, University of Illinois at Urbana-Champaign

TEAM MD: "Mapping Crop Types in Data-Sparse Regions"
- Elizabeth Dobbs, University of North Georgia
- Rishi Sinha, University of Illinois Urbana-Champaign
- Nicholas Shoemaker, University of Maryland Baltimore County

TEAM TX: "Applying Language Expertise for Enhanced Situational Awareness"
- Nathalie McGinn, George Mason University
- Yemlibike Fatkulin Haris, American Military University
- Harrison Murray, University of South Carolina
- Prof. Stanley Dubinsky, University of South Carolina and RISC mentor

TEAM NM: Growing and Projecting the STEM Pipeline
- Professor Allison Reilly, UMD and Faculty Mentor
- Calla Hughes, UMD
- Rahul Jha, University of Virginia
- Lavanya Upadhyaya, University of Illinois

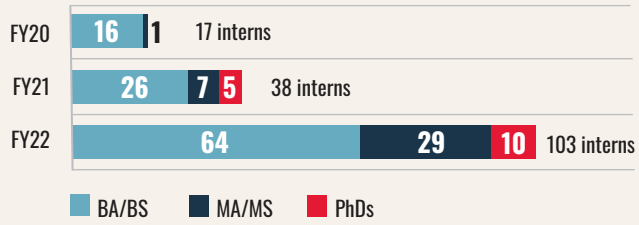
TEAM MI's final presentation, "Algorithms for Threat Detection"
- Aquia Richburg, UMD
- Courtney Teasdale, Marymount University
- Cody Arigo, UMD
- Casandra Maier, University of Georgia

RISC 2021 alum, both now full-time Faculty Specialists at ARLIS.
- Brianna Gist
- Kymani Brown

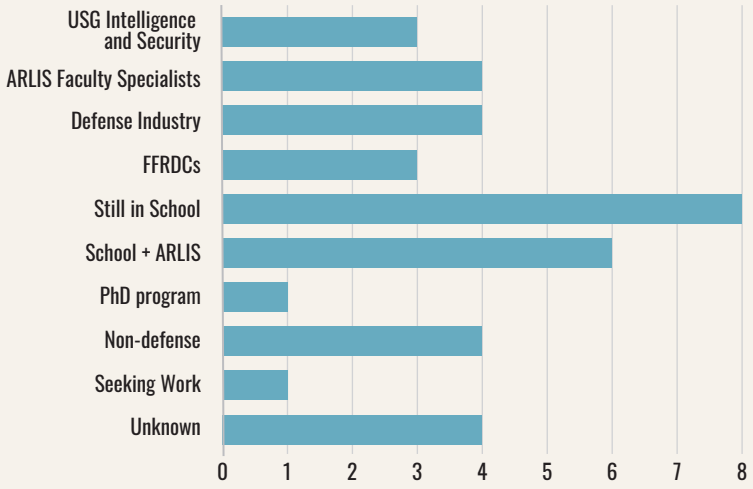
Metrics of Success

RISC has grown exponentially since its inception, from 17 students the first year to 103 in 2022. More than 35 continued working on projects into the fall, and the majority of the interns have expressed a desire to pursue careers in intelligence and security. As of October 2022, 88 interns from RISC 2022 have been successfully adjudicated for security clearances which will further facilitate those career paths.

PROGRAM GROWTH BY NUMBER OF INTERNS



RISC 2021: WHERE ARE THEY NOW



"Expanded my knowledge of what language-related opportunities there are in the IC and USG. Gave me tangible examples of possible careers and projects."

–RISC INTERN TESTIMONIAL

- Dr. Michael Maxwell, ARLIS Faculty Mentor
- Julia Sanderson, Yale University
- Kate Herrington, Michigan State University

- Brett Berlin, George Mason University research faculty and RISC mentor
- Bill Regli, ARLIS executive director
- Mithil Prasad, University of Maryland – RISC program assistant

Technical Guidance from Top Faculty

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

In 2022, 36 faculty mentors supported 40 projects, with only 13 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. 15 mentors were working with ARLIS for the first time, providing new research talent for ARLIS to engage for future intelligence and security project work.

The 2022 mentors included faculty from University of Maryland's School of Information Studies, Civil and Environmental Engineering and the Center for the Study of Terrorism and Reactions to Terrorism.

"This intern was truly excellent and went out of her way to make additional deliverables."

–PROF. CODY BUNTAIN, FACULTY MENTOR FROM UMD COLLEGE OF INFORMATION STUDIES

"The project was very interesting and the government sponsor was highly involved. The project matched the interns' level of education."

–DR. SAMUEL HENKIN, FACULTY MENTOR FROM THE UMD CENTER FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

"RISC has been the most impactful experience I have had thus far in my graduate education in applying the skills I have already learned to a real and hands-on project while simultaneously learning more through this internship and developing skills related to machine learning that will help me stand out as a candidate applying for jobs in defense and intelligence."

–RISC INTERN TESTIMONIAL

"Our project topic was so great! We were able to input into actual operational situations that occurred during the internship and it was fun to see the students get passionate about making a difference."

–DR. ANGIE MALLORY, ARLIS FACULTY MENTOR

"These interns exceeded my every expectation. They were extremely hard working and made consistent progress with minimal hand-holding."

–PROF. CHRISTOPHER METZLER, FACULTY MENTOR FROM UMD COMPUTER SCIENCE

RISC 2022 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 2022, ARLIS had the privilege to work with USG topic champions representing 18 distinct organizations within the defense intelligence and security enterprise.

- Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S))
  - Operations Security
  - Information Security
  - Insider Threat
  - Technology Protection
- OUSD(Research & Engineering)
  - Strategic Technology Protection & Exploitation
  - Small Business & Partnerships
- OUSD(Acquisition & Sustainment)
  Office of the Chief Information Security Officer
- OSD Strategic Capabilities Office
- OSD Chief Digital and AI Officer (formerly the JAIC)
- Office of the Director of National Intelligence (ODNI)/S&T
- National Geospatial-Intelligence Agency (NGA)
- Defense Intelligence Agency (DIA)
- USAF Concepts, Development, & Management (SAF/CDM)
- USAF Defense Cyber Counterintelligence Center (DC3)
- U.S. Army Futures Command
- U.S. Army Forces Command G2
- Naval Air Warfare Center - Aircraft Division

"I have always wanted a career in intelligence, but I never thought I was good enough. I don't live anywhere near the D.C. area, so I believe my location and lack of knowledge about the IC, were the largest factors keeping me from pursuing this dream. I didn't know how to even get started in this field. Being vetted for a clearance has really increased my confidence."

–RISC INTERN TESTIMONIAL

"The government sponsor was really great–clear on their needs, involved, and it was a nicely scoped project."

–PROF. KATIE SHILTON, FACULTY MENTOR FROM UMD COLLEGE OF INFORMATION STUDIES

"The program allowed me to work with an inter-disciplinary team for the first time which was a good experience for me. It also provided me with experience working on research projects outside of my area of expertise. I believe that both experiences will be good for my career prospects."

–RISC INTERN TESTIMONIAL

"Prior to the internship, I had planned to pursue my masters in the Netherlands but now after completing the internship I've shifted focus to pursuing a masters in the DC region. This was chosen in part due to my realization from the RISC program how vital networking is to my future career, and how DC is the best place in the world to facilitate that. The other reason was because of the RISC internship I now feel confident in entering the workforce due to the skills and real-world experience I gained."

–RISC INTERN TESTIMONIAL

TEAM AL: CFIUS OVER THE HORIZON FORECASTING FOR CRITICAL AND EMERGING TECHNOLOGIES
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM AZ: FOREIGN INFLUENCE ON SMALL BUSINESSES
Sponsor: OUSD(Research and Engineering) Small Business Innovation and Research Office

TEAM CA: SUSTAINING SUPPORT FOR CRITICAL AND EMERGING TECHNOLOGY PROTECTION
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM CO: UNDERSTANDING COMPETITOR EFFORTS IN BIOLOGICAL AND CHEMICAL WEAPONS AND DEFENSE R&D
Secretary of the Air Force Office of Concepts, Development, and Management

TEAM CT: DATA VISUALIZATION TO COMPARE CRITICAL TECHNOLOGIES TO THE U.S. AND CHINA
Sponsor: OUSD(Research and Engineering) Science & Technology Exploitation and Analytics

TEAM DC: MITIGATING AI BIAS IN THE DEPARTMENT OF THE AIR FORCE
Secretary of the Air Force Office of Concepts, Development, and Management

TEAM DE: HOW STRATEGIC COMPETITORS USE AI/ML
U.S. Army Futures Command Future Forces and Concepts

TEAM FL: MODELING DOWNSTREAM CONSEQUENCES OF EMBEDDED AI
Sponsor: Department of Defense Chief Digital and Artificial Intelligence Office

TEAM GA: VISUALIZING FORENSIC DATA IN OSINT KNOWLEDGE GRAPHS
Sponsor: Office of the Director of National Intelligence (ODNI) Science and Technology Directorate

TEAM IA: TRAINING AND TESTING TEXT EXTRACTION UTILITIES ON PUBLIC REPORTS
Sponsor: Office of the Director of National Intelligence (ODNI) Science and Technology Directorate

TEAM IL: MODELING DISTRIBUTED ANALYSIS WITH SOFTWARE INSTRUMENTATION
Sponsor: Office of the Director of National Intelligence (ODNI) Science and Technology Directorate

TEAM IN: DEVSECOPS IN DISTRIBUTED DEVELOPMENT TEAMS
Sponsor: Office of the Director of National Intelligence (ODNI) Science and Technology Directorate

TEAM KS: HUMAN-INTERPRETABLE ATTRIBUTION OF TEXT USING UNDERLYING STRUCTURE
ARLIS Contract with the Intelligence Advanced Research Projects Agency

TEAM KY: DATA DEVELOPMENT FOR PROJECT MAVEN
ARLIS Contract with the Office of the Undersecretary for Defense for Intelligence & Security (OSD(I&S))

TEAM LA: MACHINE LEARNING FOR SHIP IDENTIFICATION
Sponsor: Naval Air Warfare Center – Aircraft Division

TEAM MA: GROUND LEVEL IMAGE PROCESSING SEGMENT (GLIMPSE)
Sponsor: National Geospatial-Intelligence Agency (NGA) Research

TEAM MD: OPEN-SOURCE RESEARCH TO MAP CROP TYPES IN DATA-SPARSE REGIONS
Sponsor: National Geospatial-Intelligence Agency (NGA) Research

TEAM MI: ALGORITHMS FOR THREAT DETECTION
Sponsor: National Geospatial-Intelligence Agency (NGA) Research

TEAM MN: SECURE COMPUTING AND HOW TO BREAK IT: BLUE TEAM
Sponsor: Office of the Secretary of Defense Strategic Capabilities Office

TEAM MO: SECURE COMPUTING AND HOW TO BREAK IT: RED TEAM
Sponsor: Office of the Secretary of Defense Strategic Capabilities Office

TEAM NC: IMPROVING CYBER THREAT DISCLOSURES
U.S. Air Force Defense Cyber Crime Center (DC3)

TEAM NE: IMPACT OF CYBER EVENTS ON SUPPLY CHAIN AND BUSINESS OPERATIONS
Office of the Chief Information Security Officer, Cyber Warfare Directorate

TEAM NH: AMERICA'S SUPPLY CHAINS
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM NJ: PROJECT BLUE: INFORMATION SYSTEMS TO SUPPORT THE MILITARY SYSTEM SUSTAINMENT
ARLIS Contract with the U.S. Navy Naval Surface Warfare Center

TEAM NM: GROWING AND PROJECTING THE STEM PIPELINE
Sponsor: OUSD(Research and Engineering) Science & Technology Exploitation and Analytics

TEAM NV: U.S. ALLIES AND PARTNERS INTELLIGENCE AND SECURITY MODERNIZATION
U.S. Army Forces Command

TEAM NY: MEASURING THE QUALITY OF LEARNING FROM SIMULATIONS
U.S. Army Futures Command Future Forces and Concepts

TEAM OH: UNAUTHORIZED DISCLOSURES AND THE 24-HOUR NEWS CYCLE
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM OK: CHANGING MOTIVATIONS IN INSIDER THREATS
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S) Insider Threat Office

TEAM OR: INSIDER THREAT: FOREIGN TERRORISM VS. EXTREMISM
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S) Insider Threat Office

TEAM PA: HEALTHY ORGANIZATIONAL CULTURE AS A STRATEGY TO MITIGATE INSIDER THREAT
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S) Insider Threat Office

TEAM RI: SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM SC: AUTOMATION OF DECLASSIFICATION AND FOREIGN DISCLOSURE
ARLIS contract with OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM SD: INVESTIGATING APPROACHES TO MODERNIZE CLASSIFIED INFORMATION MANAGEMENT
Sponsor: Secretary of the Air Force Office of Concepts, Development, and Management

TEAM TX: APPLYING LANGUAGE EXPERTISE FOR ENHANCED SITUATIONAL AWARENESS
Sponsor: OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

TEAM UT: CHARACTERIZING IDENTITY IN A DIGITAL WORLD (CLASSIFIED PROJECT)
Sponsor: Defense Intelligence Agency

TEAM VA: INFORMATION COMPETITION SIMULATOR
ARLIS Contract with Director of Defense Research & Engineering and U.S. Special Operations Command

TEAM WI: COMPUTATIONAL CULTURAL UNDERSTANDING
ARLIS Contract with the Defense Advanced Research Projects Agency

TEAM WY: INTEGRATED FORECASTING AND ESTIMATES OF RISK
ARLIS Award with Open Philanthropy

>> TEAM AL: CFIUS Over the Horizon Forecasting for Critical and Emerging Technologies

SPONSOR AGENCY NAME
OUSD (I&S) Counterintelligence, Law Enforcement, & Security (CL&S)

SPONSORING AGENCY POC(S)
Kristoffer Buquet, Chief Technology Protection Division

RISC FACULTY MENTOR
Christopher Nissen, UMD Applied Research Laboratory for Intelligence and Security

---

Report Prepared by
Danielle Mixon | University of Maryland
Jiin Kim | University of Maryland
Lauren Shanley-DeBuse | American University

PROJECT ABSTRACT

This project aims to create a predictive analysis that can be used to determine Critical and Emerging Technology (C&ET) companies that may be susceptible to direct foreign investment or foreign-invested enterprise activity. The Foreign Ownership, Control, or Influence (FOCI) threat to our current and future C&ET is continuing to grow and becoming more invasive. This is due to direct foreign investment in U.S. companies by foreign investors and governments. Due to the ten-week time constraint, this project was scoped to focus on just two C&ET sectors, Renewable Energy and Space Technology. This project is a proof of concept for predictive analysis. The project's three-step methodology demonstrates an automated discovery process for companies working on C&ET, a rank order process to evaluate companies' potential susceptibility to foreign investment, and a risk assessment. The goal of this predictive analysis is to decrease the time and effort required to identify C&ET companies at risk of FOCI. In order to accomplish this task, manual research methods and processes have been augmented with a number of analytical tools. The result is a hybrid manual and automated predictive analysis that utilizes data mining techniques, statistical programming, and machine learning. The predictive analysis identifies companies that are susceptible to foreign compromise and evaluates their respective levels of risk. Due to the hybrid format, the predictive analysis is repeatable. It also has the potential to be scaled to evaluate larger sets of data more efficiently.

>> TEAM FL: Modeling Downstream Consequences of Embedded AI

SPONSOR AGENCY NAME
OUSD(I&S), Office of the Chief Digital and AI Officer (CDAO)

SPONSORING AGENCY POC(S)
LtCol Brian Wooley, Dr. Chad Beiber

RISC FACULTY MENTOR
Dr. Joshua Poore, UMD Applied Research Laboratory for Intelligence and Security

---

Report Prepared by
Michael Cocita | University of Maryland
Austin Cohen | University of Wisconsin
Aidan Kurz | University of North Texas

PROJECT OVERVIEW

Model downstream consequences that embedded AI had on a system.

Objectives:
- Learn the entities and connections between entities in the system of interest
- Model the system with accuracy by confirming with sponsor through briefs and interviews
- Apply System Theoretical Process Analysis (STPA) towards the system

General Findings
- Components within a system can be many and difficult to map out.
- Applying STPA helps to see in detail what each component contributes from the actions they are capable of. We found that these actions can cause issues implicitly to other components not directly linked to the component performing the action.

These findings are very important, as they support the team's belief that STPA was the proper method to use for risk and hazard analysis. The findings allowed the team to observe that by applying STPA early within the planning process, potential issues are identified much earlier allowing for proper adjustment of the project plan. The team found by applying the process to multiple use cases that STPA applies to a wide range of fields allowing it to be generalized and applicable for all fields of research, industries, and project planning.

>> TEAM LA: Machine Learning for Ship Identification

SPONSOR AGENCY NAME
Naval Air Warfare Center -- Aircraft Division

SPONSORING AGENCY POC(S)
Charles Rea, Andrew Pontzer, and Theresa Shafer

RISC FACULTY MENTOR
Prof. Christopher Metzler, UMD Computer Science

Report Prepared by
Ethan Adams | University of North Texas
Rushil Joshi | University of Maryland

PROJECT GOALS

Overarching Goal of this Project:
Utilizing neural networks, the project aims to improve ship detection by using a light-weight algorithm that can be implemented on UAVs for real time detection.

Additional goals:
Develop novel training frameworks that can learn to segment ships using only efficiently-collected, weakly-supervised data via the technique of point-annotated segmentation.

Why the Intelligence and/or Security Community should care:
The rapid advancement of neural networks and artificial intelligence has made it possible to perform previously infeasible tasks, such as monitoring the entire US coast for potential threats via the air. By being able to detect objects of interest in real time on a lightweight device, operators can make quicker decisions and command posts can have stronger analysis of what is transpiring out in the field.

>> TEAM MA: Ground Level IMage Processing SEgment (GLIMPSE)

SPONSOR AGENCY NAME
National Geospatial Intelligence Agency (NGA)

SPONSORING AGENCY POC(S)
Chris Mikrut

RISC FACULTY MENTOR
Prof. Alan McMillan, University of Wisconsin

Report Prepared by
Matthew Traver | James Madison University
Tyler Houser | George Mason University
Nathan Bickel | University of South Carolina

PROJECT ABSTRACT

GLIMPSE is an NGA geolocation tool that determines where outdoor photographs were taken by analyzing ridgelines within their backgrounds. Because GLIMPSE is an intensive pipeline that can only handle a limited number of images per day, our goal was to create and deliver an interest module that would help detect when text and objects of interest are within an image, allowing for their prioritization.

This new interest module adds an optical character recognition (OCR) model and an object detection model. The OCR model helps to recognize when text is present in an image and the language of the text. The object detection model detects when firearms (and individuals) are present in an image. Both models will help the interest module prioritize images relevant to national security and those more easily geolocated. In addition to creating the interest module, we provided the NGA with a conceptual framework to help combat human trafficking at various hotel chains using indoor geolocation.

Future work should focus on developing an open-source OCR model to detect text more accurately, developing additional object detection models for other objects of interest, and integrating indoor geolocation capabilities into the pipeline to combat human trafficking and other relevant phenomena.

>> TEAM NE: Impact of Cyber Events on Supply Chain and Business Operations

SPONSOR AGENCY NAME
OUSD(Acquisition & Sustainment) Cyber Warfare Directorate

SPONSORING AGENCY POC(S)
John Garstka, Director for Cyber in the Office of the Chief Information Security Officer, A&S; Colonel William E Wade, Deputy Director for the Cyber Warfare Directorate

RISC FACULTY MENTOR
Dr. Charles Harry, University of Maryland School of Public Policy

---

Report Prepared by
Avery Borens | Pennsylvania State University
Emily Klomparens | University of Maryland
Ryan Thenhaus | University of Wisconsin

PROJECT ABSTRACT

Our project deals with estimating and analyzing the costs of cybersecurity for small business DoD contractors. NIST SP 800-171 mandates a certain level of cybersecurity standards that must be upheld to work with the DoD. Though cybersecurity is important, the vast majority of small businesses will struggle to afford the costs of adhering to the NIST standards. According to our estimations, the cost-per-employee is too high for small businesses that must work with few employees and modest revenue. The NIST SP 800-171 standards may force many contractors to cease doing business with the DoD. We have also identified many factors affecting the economics of cybersecurity, including geography, demand for labor, and managed service providers. The importance of our project stems from the fact that a majority of DoD contractors and subcontractors can be classified as "small businesses". Although exact numbers for DoD contractors are not known, companies under 1,000 employees make up 99.9% of the US economy as a whole. These proportions are likely indicative of the Defense Industrial Base distribution as well. As a result, steps should be taken to avoid imposing these large and detrimental costs upon such a significant portion of US defense contractors.

Why the Intelligence and/or Security Community should care:
The intelligence community should care because there is a lack of research and consideration about the economic factors of small business cybersecurity (the economic side is often overlooked). Inadequate small business cybersecurity can cause national security risks and increase vulnerabilities, especially among defense contractors. Current NIST standards may force small businesses out of the Defense Industrial Base due to prohibitive costs.

>> TEAM NV: U.S. Allies and Partners Intelligence and Security Modernization

SPONSOR AGENCY NAME
U.S. Army Forces Command G2

SPONSORING AGENCY POC(S)
James Johnson

RISC FACULTY MENTOR
Dr. Samuel Henkin, UMD Center for the Study of Terrorism and Responses to Terrorism (START)

Report Prepared by Team NV
Stephanie Lizzo | Sciences Po (FR)
Jasmine Phillips | Leiden University (NE)
David Winter | Texas A&M University

PROJECT ABSTRACT

Driven by recent geopolitical events and technological advances, U.S. allies have begun developing their defense and intelligence capabilities, independent of U.S. funding and participation. By eschewing U.S. cooperation, these partners might develop programs or tools incompatible with U.S. systems or threaten U.S. operations abroad. Through open-source research and interviews with subject matter experts (SMEs), we evaluated U.S. allies' modernization efforts, their state of development, their interoperability with existing and future U.S. systems, and whether they match or outstrip U.S. capabilities. European-NATO countries were the focus of this research. The primary finding was that no ally is close to outpacing the U.S. regarding innovation projects; the more salient concern is that allies cannot keep pace and will be left behind in the modernization race. Despite the strict interoperability standards by NATO, several country-specific modernization efforts may not be compatible with the U.S. However, many are too early in the development process to assess accurately. Additionally, the researchers concluded that existing data- and intelligence-sharing agreements were effective but can be modified to reflect novel technological and geopolitical developments.

Why the Intelligence and/or Security Community should care:
By developing a comprehensive, nuanced understanding of the ongoing efforts of U.S. allies and partners, the U.S. IC will be better positioned in the long run. It can keep an eye on countries that might be developing competing technologies or systems and adjust their own short- and long-term strategies accordingly. Our project encourages a reevaluation of current U.S. programs to redirect research funding, a renewed emphasis on emerging technologies, or emphasize the importance of the "human factor" in this modernization.

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

SPONSOR AGENCY NAME
U.S. Army Futures Command

SPONSORING AGENCY POC(S)
LTC Mark Askew, LTC Nathan Strickland

RISC FACULTY MENTOR
Dr. Angie R. Mallory, Dr. Nick B. Pandža, UMD Applied Research Laboratory for Intelligence and Security

---

Report Prepared by
Ethan Morrow | University of Illinois at Urbana-Champaign
Lillian Stout | Princeton University

PROJECT ABSTRACT

Concerns about the validity of wargaming results have become prominent in recent years. This is likely due, in part, to divergent perspectives on how to design an effective wargame. To address this divergence, this handbook will attempt to standardize the processes of wargame design and evaluation.

Drawing from best practices of narrative and scientific wargaming, as well as those from social science, this work presents a guide for wargamers that combines logistical and theoretical insight. In addition, this handbook introduces several resources that can facilitate the process of designing and evaluating wargames and their results. It is hoped that these attempts to standardize the field will improve the validity of wargame results and, in turn, promote confidence in the wargaming process. The acceptance and application of valid results will not only move the field of wargaming forward, but will also save lives and promote the realization of the nation's goals.

Why the Intelligence and/or Security Community should care:
The wargaming community is currently undergoing a shift from wargaming as a narrative-based thought experiment to a means of developing and empirically testing new concepts and capabilities (science-based). However, some wargame designers and analysts are unaware of the best practices in this emerging landscape of wargaming. In addition, senior leaders tasked with overseeing these wargames are often not familiar with the intricacies of the wargaming process. Ultimately, the wargaming process lacks structure and uniformity. The lack of standardization parameters leads to issues in the quality of wargame design and evaluation alike. This project provides the wargaming field with the necessary, preliminary tools it needs to develop games that produce results of high validity.

>> TEAM OH: Unauthorized Disclosures and the 24-Hour News Cycle

SPONSOR AGENCY NAME
OUSD(I&S) Counterintelligence, Law Enforcement, & Security (CL&S) PHYSEC&OPSEC USG

SPONSORING AGENCY POC(S)
Erica S. McLennan, Chief of DoD Operations Security (OPSEC)

RISC FACULTY MENTOR
Dr. Natalie M. Scala, Towson University

Report Prepared by
Taylor Seaman | George Washington University
James Raymond | University of New Haven
Sara Freedman | Virginia Polytechnic Institute

PROJECT GOALS

Overarching Goal of this Project:
Team OH conducted research through reliable sources focusing on intentional unauthorized disclosures (UD) of protected information to the media. This endeavor included a thorough review of the problem, examination of causes and motivations for UDs, and development of alternatives for mitigating the issue. The research resulted in ten Operations Security (OPSEC) recommendations organized into four major themes with implementation advice for the Department of Defense (DoD) to adopt to reduce the risk of UD, including innovations to enhance current best practices in the field.

Why the Intelligence and/or Security Community should care:
As the media and news cycles become increasingly influential, unauthorized disclosures develop into more pressing threats to US national security. UDs cost the US government time, money, and valuable information. Prevention and mitigation is key to protecting our nation against adversaries. Information secured at a higher classification (e.g. Top Secret) or lower classification (e.g. CUI) can be equally vulnerable to disclosure to our adversaries. Foreign intelligence services and terrorist organizations have been known to aggregate sensitive information that can be harmful to national security when viewed as a whole. Therefore, all forms of sensitive information, including both classified and CUI, should be protected with the utmost vigilance.

>> TEAM RI: Safeguarding Controlled Unclassified Information

SPONSOR AGENCY NAME
USOD (I&S) Counterintelligence, Law Enforcement, and Security (CL&S)

SPONSORING AGENCY POC(S)
Michael Russo, Chief, Information Security Policy
Peggy Ushman, Information Security Analyst

RISC FACULTY MENTOR
Prof. Katie Shilton, University of Maryland, School of Information Studies

---

Report Prepared by
Adams Awasum | University of Maryland
Kendall Snyder | University of Maryland
Taylor Codispoti | Pennsylvania State University

PROJECT ABSTRACT

Controlled Unclassified Information (CUI) is a broad category of information security that refers to many different types of sensitive, but not classified, information. While the way CUI has been treated, labeled, and disseminated has been updated in recent years, there still exists confusion over what information truly classifies as CUI, the types of CUI, and how CUI should be handled. In an effort to assist in alleviating these issues, our team reviewed the CUI Registry and cataloged examples of each category of CUI (as well as warning statements and dissemination controls). As we dissected the registry, our team also conducted a thorough review of CUI documents, noting major pitfalls in the literature and crafting potential fixes to identified problems. We concluded our research by analyzing the consistent issues we were coming across and working with our government sponsor to better suit the registry for the needs of the Department of Defense (DoD). The work on this project will improve the way the DoD is able to assess and analyze issues of CUI to better protect many different types of sensitive information.

Why the Intelligence and/or Security Community should care:
The ability to handle and identify CUI makes this whole project extremely important for the security community to be aware of. Our project strives to make it easier for those in specific departments to quickly and affectionately determine how to properly handle CUI. By accumulating the definitions and including examples, the entire CUI community can be better understood by those in the government and information would be better handled. The system of gathering all the information can then be used to gather information regarding documents with higher classification.

>> TEAM VA: Information Competition Simulator

SPONSOR AGENCY NAME
ARLIS contract with U.S. Special Operations Command

RISC FACULTY MENTOR
Matt Venhaus, Dr. Angie Mallory, UMD Applied Research Laboratory for Intelligence and Security

---

Report Prepared by
Taylor Gordon | Howard University
Nurul Haya | University of Maryland
Autumn Perkey | University of Maryland
Anna Prince | Georgetown University

PROJECT ABSTRACT

ICS seeks to model the spread of information in a wargame-like environment. While traditional wargaming approaches facilitate freeplay ***or*** realism, ICS integrates both by tailoring the gaming environment to a real-world population. This innovation is very important for the information era, where traditional wargames often fail to capture the complex psychological and group dynamics that are amplified by mass-communication and mass-connection.

ICS is a large-scale, complex, and highly interdisciplinary project. Thus, our approach and findings have varied significantly by team. Those focusing on identity have conducted in-depth research into our target population. Those focusing on model rules have adapted theoretical frameworks into mathematical calculations. Those focusing on user interface have aimed at creating an intuitive interface design for influence-based wargames. Within six months, we anticipate a functional model that enables users to conduct a wargame. ICS is developed in collaboration with teams from the University of Florida and the University of South Carolina.

Why the Intelligence and/or Security Community should care:
Existing training, experimentation, and wargaming environments account for neither real human behavior nor the demographic specifics of the target population. Thus, prior models may sacrifice precision, interactivity, true-to-life behavioral consequences, or configurability. ICS addresses these shortcomings with modeled populations that, based on careful research of both the target population's demographics and other applicable theories in social psychology, mirror their real-life counterparts. This more real-to-life, behavior-based approach allows users to rigorously test strategies for both conducting and counteracting real-world influence campaigns. In short, ICS will serve as a valuable educational and training tool for the defense community, as well as a guide for policy and strategy formation in the information era.

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