APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

ARLIS Program Reviews, v3.0 Series 2021

Day 1 – Tuesday 4 May 2021

Tuesday 4 May	
0900 – 0915	**Introduction and Overview of the Day**
0915 – 0945	**ARLIS: Enabling the Intelligence Edge**
0945 – 1135	**Cognitive Security and Operations in the Information Environment**
1135 – 1215	Lunch break
1215 – 1430	**Applied AI, Autonomy, and Augmentation (AAA)**
1430 – 1440	Break
1440 – 1530	**Human Performance: Augmentation**
1530 – 1645	**Human Performance: Aptitude**
1645 – 1700	Wrap-Up

Wednesday 5 May	
0900 – 0915	Overview of the Day
0915 – 0945	**Computational Infrastructure**
0945 – 1035	**Data Curation and Resource Building**
1035 – 1045	*Break*
1045 – 1125	**Testbeds and Subject Matter Expertise**
1125 – 1210	**Managing & Mitigating Insider Risk**
1210 – 1300	*Lunch break*
1300 – 1410	**Acquisition and Industrial Security**
1410 – 1445	**Augmented Collective Intelligence**
1445 – 1500	*Break*
1500 – 1530	**FY22 Internal Research & Development Projects**
1530 – 1540	**The Intelligence & Security University Research Enterprise Consortium**
1540 – 1610	**Training and Workforce Programs**
1610 – 1630	Wrap-Up

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY
UNIVERSITY OF MARYLAND

Time	Description
Tuesday 4 May	
0900 – 0915	**Introduction and Overview of the Day** Pamela Castleberry and Erin Fitzgerald
0915– 0945	**ARLIS: Enabling the Intelligence Edge** Executive Director William Regli
0945– 1135 (110 minutes)	**Cognitive Security and Operations in the Information Environment** • Portfolio Overview and Primary Tasks, Michael Bunting, 30 • Computational Social Science, Anton Rytting, 20 • The Role of Emotions in Adversarial Information Campaigns, Susannah Paletz, 20 • Sociotechnical Analyses to Address the COVID-19 Pandemic, Ruthanna Gordon, 10 • Dark Uses of Immersive VR for Disinformation and Adversarial Manipulation, Ewa Golonka [IRAD], 10 • *INfluence Campaign Awareness and Sensemaking, Devin Ellis and Amanda Towler, 10
1135 – 1215	*Lunch break*
1215 – 1420 (125 minutes)	**Applied AI, Autonomy, and Augmentation (AAA)** • Portfolio Overview and Primary Tasks, Craig Lawrence, 30 • Anticipatory Ground-Level Imagery Analytics, Michael Pack, 30 • *Autonomy Application & Engineering Exploratorium, Laurel Miller-Sims, 30 • Integrated Discovery of Emerging and Novel Technologies, Michael Maxwell, 15 • There is no AI in Team: A Multidisciplinary Framework of Features for AIs to Work in Human Teams, Susannah Paletz [IRAD], 10 • AI Engineering Initiative, Craig Lawrence, 10
1420 – 1430	*Break*
1430 – 1515 (45 minutes)	**Human Performance: Augmentation** • Portfolio Overview, Polly O'Rourke, 5 • Targeted Neuroplasticity Training (TNT), Polly O'Rourke, 30 • Examining the Underpinnings of Creativity, David Martinez, 10 • Unbiasing Analysts: Reducing cognitive biases in intelligence analysts with noninvasive peripheral nerve stimulation, David Martinez [IRAD], 10
1515 – 1630 (45 minutes)	**Human Performance: Aptitude** • Portfolio Overview: Susan Campbell, 5 • Computer Language Aptitude Battery & Proficiency Testing, Nick Pandža, 20 • Cyber Aptitude and Talent Assessment (CATA), Susan Campbell, 10 • High-Level Language Aptitude Battery (Hi-LAB), Ewa Golonka, 10
1630 – 1645	Day 1 Wrap-Up

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

UNIVERSITY OF MARYLAND

Wed. 5 May	
0900 – 0915	Overview of the Day
0915 – 0945	**Computational Infrastructure** Joseph Kelly and John Romano. 30
0945 – 1035 (50 minutes)	**Data Curation and Resource Building** • Portfolio Overview, Michelle Morrison. 5 • *Support to IARPA MATERIAL (Machine Translation for English Retrieval of Information in Any Language), Michelle Morrison. 10 • *Support to DARPA KAIROS: Corpora of Annotated Events Represented Under Schemas, Aric Bills. 15 • *Support to IARPA BETTER (Better Extraction from Text Towards Enhanced Retrieval), Michelle Morrison. 20
1035 – 1045	*Break*
1045 – 1125 (40 minutes)	**Testbeds and Subject Matter Expertise** • GATR (Mantra) - PAI/CAI Data Analysis, Joseph Kelly. 10 • *FAAST: Food & Agricultural Assurance & Supply chains Testbed, Polly O'Rourke. 10 • *IV&V of the AISS Program, Warren Savage. 10 • EW Study into broader Cyber-Electromagnetic Activities, Austin Branch. 10
1125 – 1210 (45 minutes)	**Managing & Mitigating Insider Risk** • Portfolio Overview and Primary Tasks, Kelly Jones. 30 • Understanding the Commercial Landscape for Insider Threat Detection, Dinesh Manocha. 10 + 5 Q&A
1210 – 1300	*Lunch Break*
1300 – 1410 (70 minutes)	**Acquisition and Industrial Security** – TBC • Portfolio Overview and Primary Tasks, Thomas Hedberg. 30 • ARLIS Support for 5G Initiatives, Wayne Phoel. 20 • Emerging Technologies, WMD, and Strategic Trade Controls, Nancy Gallagher. 20
1410 – 1445 (35 minutes)	**Augmented Collective Intelligence** – TBC • Portfolio overview, Adam Russell. 5 • Crowdsourced Security & Intelligence Forecasting Tool, Jana Schwartz. 15 • SANDS2: Supporting A Navy Decision Science Strategic Framework, Adam Russell. 15
1445 – 1500	*Break*
1500 – 1530 (20 minutes)	**FY22 Internal Research & Development Projects** • Automatic Identification of Narratives, Brook Hefright. 10 • Identifying and Tracking Russian Operations in the Information Environment in Central Asia, Marilyn Maines. 10, + Q&A
1530 – 1600 (30 minutes)	**Intelligence & Security University Research Enterprise Consortium,** Erin Fitzgerald
1600 – 1630 (30 minutes)	**Training and Workforce Programs** • The Technology and Law Academy, Harvey Rishikof. 10 • Research for Intelligence & Security Challenges (RISC) Internship, Erin Fitzgerald
1630 – 1645	Wrap-Up

Rules of (zoom) Engagement

- Everybody on MUTE (except the speaker)
- Event is *mostly* transmit-only
- Please submit questions via ZoomGov Chat, preface questions in the chat with "QUESTION:"
- Use the chat session to interact with each other
- Regli & Russell & Erin & Pamela: your moderators for the session
- Take note of slides/speakers you wish to follow-up with, introductions will be facilitated if needed

Desired Outcomes of the Program Reviews

- Create ARLIS-wide situation awareness
- Create opportunities for campus situation awareness
- Promote collaboration, ideation, and new program concepts
- Identify cross-cutting themes
- Identify big wins, successes, and accomplishments
- Communicate ARLIS capabilities to stakeholders
- Produce materials for annual report, web site, etc
- Answer the Heilmeier for each project: what are we trying to do?
  What's the new idea? Transition/Impact?

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

ARLIS: Enabling the Intelligence Edge

A University Affiliated Research Center for the Intelligence and Security Communities

William Regli
Executive Director, Applied Research Laboratory for Intelligence & Security
Professor of Computer Science
The University of Maryland at College Park

A Reflection: A UARC's Objectives

From: ***Engagement Guide Department of Defense University Affiliated Research Centers***, April 2013

- UARCs were established May 1996 to ensure that essential engineering and technology capabilities of particular importance to the DoD are maintained
- Develop and maintain essential government-defined research, development or engineering capabilities and provide those to DoD through a long-term strategic relationship.
- Develop a strategic relationship with their sponsor that gives them knowledge of their sponsor's needs and access to their information;
- Operate in the public interest as strategic partners with their DoD sponsors, rather than in the interest of corporate shareholders, and conduct its business in a manner befitting its special relationship with DoD, combining technical excellence with objectivity.
- Respond quickly to sponsor needs, serving as subject matter experts that function as independent, trusted advisors and honest brokers, answerable only to their DoD customers.

Origin Stories

MIT's Lincoln Labs (FFRDC)

- Est. 1940 as the "Rad Lab"
- Tizard Mission → cavity magnetron → radar and air defense

Today: Radar, space, coms, etc

JHU APL (UARC)

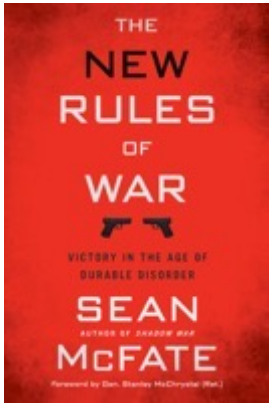
- Est. 1942
- Tizard Mission → doppler radar fuses → VT proximity fuses

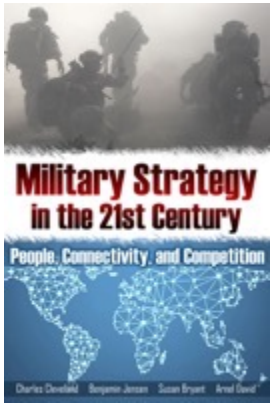
Today: guidance, space, cyber, systems engineering, etc.

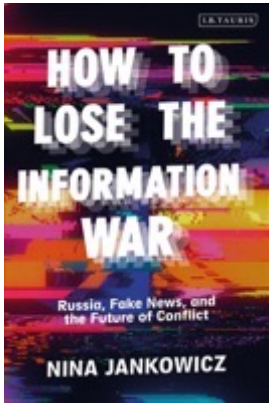
Core Competencies -->	#1	#2	#3	#4	#5	#6
Johns Hopkins Univ Applied Physics Lab (APL)	Strategic systems testing/evaluation	Submarine security	Space engineering	Guidance	Air defense	Information Technology
Pennsylvania State Univ Applied Research Lab (ARL)	Undersea Guidance	Undersea Control	Propulsion	Communications systems	Materials	
University of Texas Applied Research Lab (ARL)	Underwater acoustics	Sonar systems	Underwater systems	Electromagnetic research	PNT	C4I
University of Washington Applied Physics Lab (APL)	Remote sensing	Ocean Physics	Undersea warfare	Submarine & sonar studies	Signal & image processing	
University of Hawaii Applied Research Lab (ARL)	Ocean Research	Astronomy	Sensors & Remote Sensing	Renewable Energy	Opto-Eletrical Systems	
Georgia Tech Georgia Tech Research Institute (GTRI)	Systems Engineering	Cybersecurity	Sensors, Weapons, EW	Threat Systems	Electromagnetics	Autonomous Systems
University of Southern California Institute for Creative Technology (ICT)	Virtual Reality	Scenario Generation	Content Creation	Computer Graphics	Sound Design	Evaluation
MIT Institute for Soldier Nanotechnologies (ISN)	Nanomaterials research	Structural Materials	Energy & Power	IT for Soldier Systems	Next-gen Electronics	Warfighter Medicine
UC Santa Barbara Institute for Collaborative Biotechnologies (ICB)	Biotechnology	Bio-materials	Cognitive Neuroscience	Synthetic Biology	Multi-Scale Modeling of Bio	
Utah State Univ Space Dynamics Lab (SDL)	Space-based platforms	Sensors, data collection, & analysis	MDA research	Data analytics transition		
University of Maryland (ARLIS) Applied Research Laboratory for Intelligence and Security	Language, Linguistics & Human Culture (Social Science)	Semantics, computational & socio-linguistics (Sensemaking)	Analysis & Critical Thinking (AI & Augmentation)	RDT&E in Cog. Science, Neuroscience, Communication	RDT&E in AI, KR, data mining, HCI, big data, cyberinfrastructure	
Stevens Institute of Technology Systems Engineering Research Center (SERC)	Systems engineering	Acquisition	Security	Digital Engineering	Systems Theory	
University of Nebraska National Strategic Research Institute (NSRI)	Nuclear Detection & Forensics	CBNE Detection	Counter WMDs	Consequence Management	Space/Cyber/Telcom Law & Policy	

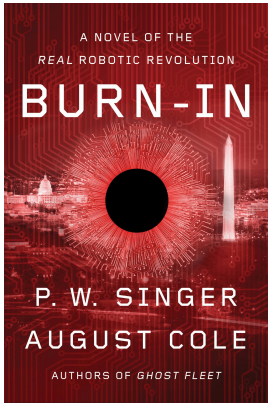
From the electro-magnetic to the information spectrum
From kinetic warfare to the Human Domain

Conflict among great powers is an "all of nation" and "whole of government" challenge; new science, technology, and capabilities are needed.









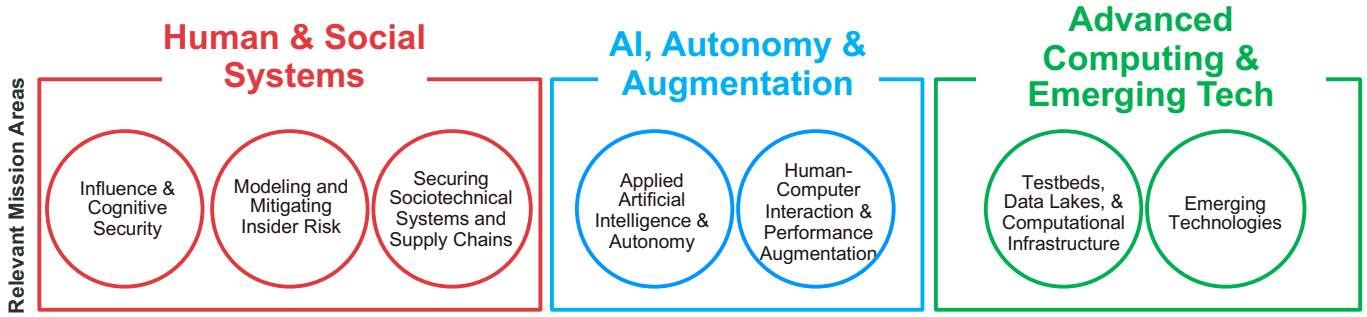
New threat surfaces emerging from complex, digitized human-technology interactions increasingly challenge our capabilities to defend the US, our people, our societal systems, and our allies.

New thinking, skillsets, and RDT&E are required for the Information Spectrum & the Human Domain.

About ARLIS

- The **only** UARC with core competency in human and social systems
- The **only** UARC reporting to the Intelligence & Security communities
- Intelligence & Security mission areas include:

  Information/Influence; Insider Risk/Trust; Vetting; Trusted Autonomy; Human/Machine Teaming; Technology Protection; CounterIntelligence, Acquisition & Supply Chains; Language & Cultural Analytics; Wargaming; Data Curation/Stewardship; Personnel Pipeline.
- Manages the **Intelligence and Security University Research Enterprise (INSURE)** academic consortia (sim model to Stevens' SERC UARC)
- Operates unique facilities in the National Capital Region (NCR)



Selected Accomplishments in 2020

- >$40M in awards; FVEY activities (AUS, UK); >90% staff growth; major new launches (DNI, DDR&E, DARPA, NGA); personnel pipeline programs
- >75 people, >45 PhDs, mostly TS/SCI, in disciplines such as psychology, linguistics, computer science, anthropology, social science, information science, human-machine interaction, systems engineering, manufacturing
- >65 active projects, from unclassified to SCI; from basic research to systems development and operational support; **6 major IV&V/T&E efforts**
- Deploying cyber-infrastructure, provisioning from unclass to CUI to SAP
- Major national leadership in key ARLIS mission areas:
  - Operations in the Information Environment (Belt & Road, regional work, DARPA);
  - Supply Chain/Counterinteligence (5G, insider threat, vetting);
  - Applied Autonomy and Human-Machine Integration (NGA, SCO, MAVEN);
  - Transition of **IC Prediction Market** from IARPA for broad use

Other highlights from the past 12 months

- CATA: UMD IT Invention of the Year
- Big Wins
  - INCAS: DARPA T&E Award
  - AISS: DARPA T&E Award
  - Vienna: DARPA T&E Award
  - EW Study: PEO STRI
  - 5G: DDR&E
- Workshops
  - 5G, AI, Insider Threat
- Phoenix Challenge 2.0
- IARPA BETTER
- USN Columbia Class
- INSURE
- AIRRIC/RISC
- TLA 2.0
- ICPM transition to I4C!
- ARLIS PEOPLE!
- Security Team
- Financial Model
- Contract vehicles and ceiling
- NAS/NAE engagement

ARLIS Mechanics

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Ideation & Program Development

Team development & execution

Products & Deliverables

Mission/Operational requirements/needs

Outcomes & Transition

Gov't resources, datasets, and operators

Nature of ARLIS's Work:

- Applied & Use-Inspired Restricted Research
- **Trusted Agent**
- Contracts (not grants)
- Fixed duration
- Specific deliverables

TRL 1	TRL 2	TRL 3	TRL 4	TRL 5	TRL 6	TRL 7	TRL 8	TRL 9
Basic principles observed and reported	Technology concept and/or application formulated	Analytical and experimental critical function and/or characteristic proof of concept	Component and/or validation in laboratory enviornment	Component and/or validation in relevent environment	System model or prototype demonstration in a relevant environment	System prototype demonstration in an operational environment	Actual system completed and qualified through test and demonstation	Actual system proven through successful operations

ARLIS as Trusted Agent vs traditional Performer

Starts with the Gov't

- Project emerges from a relationship and ARLIS mission/capabilities
- Products to be defined by the Gov't; refined continually
- Job of PI is to manage the gov't and adjust to ensure gov't success
- Gov't may change the PI; ARLIS may change the PI to reduce risk
- Focus is on the mission and its success
- Project scope, scale, timeline is aligned with mission and its duration
- ***At the ARLIS UARC, this is always the preference!***

Ways to think about ARLIS: a GOCO or "USG Laboratory" operated by The University of Maryland

Starts with an ARLIS/internal idea

- Requires **PPP**: People, Project, Patron
- Project emerges when a PI (ARLIS people)
  - Has an idea/concept for a project
  - Has a relationship with a patron
  - Patron has funds and mission need
- Successful PIs
  - have "shovel ready" new ideas (whitepapers) all the time (out of IRAD?)
  - are constantly looking for relationships with sponsors that have funds and mission need
  - are constantly refining ideas based on feedback from possible sponsors and mission stakeholders
- Funded work is driven by the proposal concepts produced by the PI and the team
- Outcomes may be adjusted by USG, but are usually driven by original ideas from PI/team
- Needed in order to build core competency & CVs

INSURE

The **IN**telligence and **S**ecurity **U**niversity **R**esearch **E**nterprise

- INSURE is a key aspect of the ARLIS enterprise
- Mission-area leads, PIs and ARLIS staff need to make an effort to get to know these institutions and develop relationships
  - Do a virtual visit, give a talk, host a talk, do a tech round table, etc
- Where expertise is not available locally, reach out
- Where S&T discriminators are not adequate locally, reach out
- ARLIS has POCs at each institution with whom one can network
- The benefits of involving INSURE institutions outweighs the extra work involved to build and manage distributed teams
- ARLIS is responsible for the success of INSURE

About INSURE

- Economic Statecraft Program, led by TAMU Bush School and funded by USAF CDM
- Human-Machine Ecosystem Laboratory, led by TAMU System and funded by NSA
- Expanding Applications for AI Automation and Augmentation including Insider Risk work led by UMD START and imagery analysis algorithms led by TAMU, funded by USAF CDM
- Five pilot projects funded by DDR&E HBCU Program Office
  1. 5G Technology Assessment -- Morgan State and Howard
  2. Machine Learning Experimentation -- UDC
  3. Cyber-Assessment of AI/ML Tools -- Howard and Morgan State
  4. AI/ML Systems Engineering Workbench – Howard and Morgan State
  5. ChatBot Testbed – Howard, Morgan State, and UDC
- INSURE Value Proposition
  - Participation in the role as trusted performer for the USG
  - Academic alignment and growth to support the core competencies
  - Expansion of use-inspired and applied research opportunities
  - Regular interaction with S&T leadership of IC agencies

Directly tied to ARLIS mission activities & sponsors

"no matter who you are, most of the smartest people work for someone else."
-- [Bill] Joy's Law

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

ARLIS Engagement with the Services

- Army PEO STRI/TSMO
- Naval Information Warfare Center-Atlantic
- Army 1st Special Forces Command
- USMA Army Cyber Institute
- Army Special Operations Command (USASOC)
- ARL, AFRL, ONR
- Army Cyber Command
- Coast Guard HQ - Materiel Readiness
- SOCOM AT&L
- SOCOM JCOG
- CyberCommand
- NAVSEA PMS 397
- US Navy, ManTech Office; USAF ManTech Office
- 10th Fleet Navy Cyber
- NIWC-PAC
- NAWCAD
- NSWC Carderock
- SAF/CDM
- USAF 517th Training Group at DLIFLC
- USAF LREC Program
- SAF/A6
- AFCLC
- HAF/A1D-LREC,
  AF Language, Regional Expertise and Culture Office

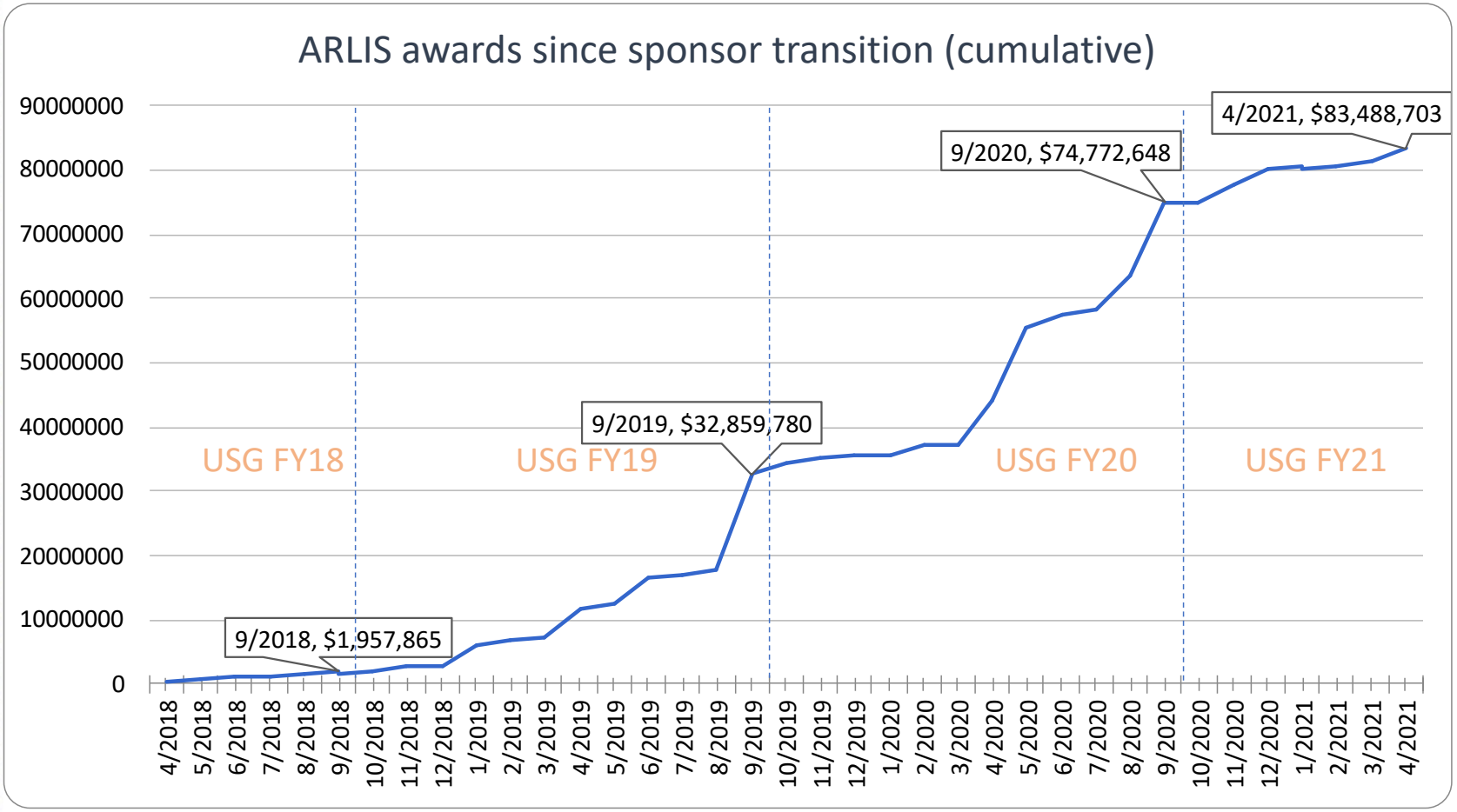
Engagement with the Intelligence and Security communities

- OUSD(IS)
  - Multiple
- DNI
  - S&T, Supply Chain, NIU
  - IARPA
- NGA
- CIA
- DIA
- DCSA
- NCSC
- NCCA
- FBI
- NDU
- NSA

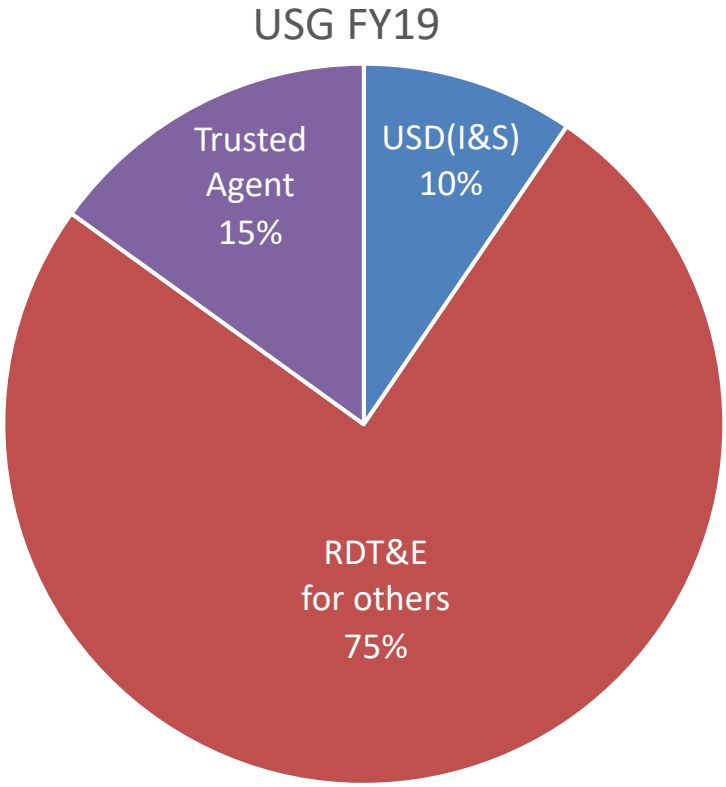
Additional ARLIS Engagements

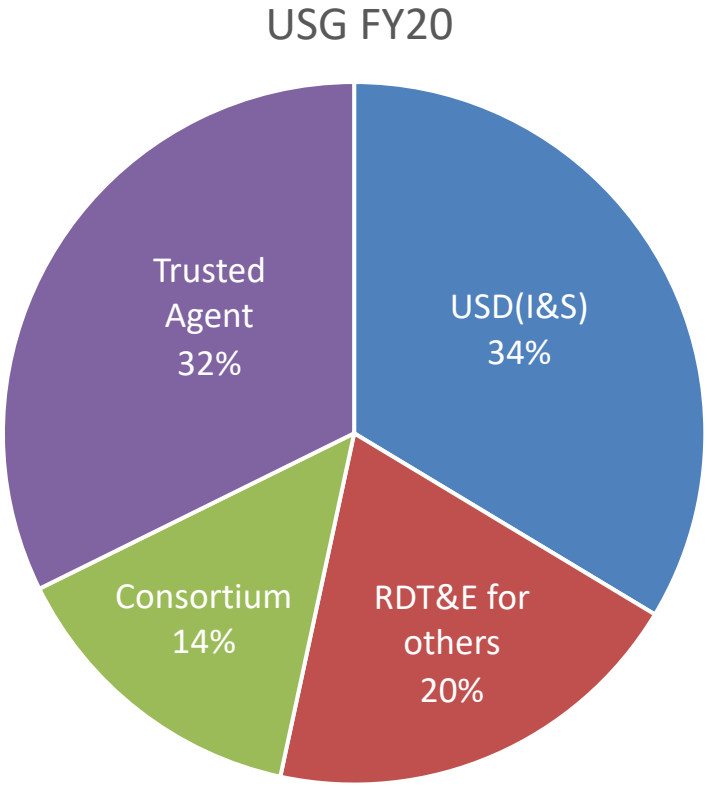
- MITRE — Deliver Uncompromised, FVEYs, Insider Risk, IO/IW, CogSec
- RAND — IO/IW, CogSec
- JHU APL — Cyber Invictus, IO/IW, CogSec
- PSU ARL — Acquisition security, Counterintelligence, Vetting
- MIT LL — IO/IW, CogSec
- SERC — Acquisition security

- UMD: — BSOS (START, Geo), ENG (ECE, ISR, CATT, MechE), CMNS (UMIACS, CS), SPP, AHU (NFLC), ISchool
- FVEY: — Joint AUS-ARLIS Information & Influence Seminar Series


ARLIS awards since sponsor transition (cumulative)
90000000
80000000
70000000
60000000
50000000
40000000
30000000
20000000
10000000
0
USG FY18
USG FY19
USG FY20
USG FY21
9/2018, $1,957,865
9/2019, $32,859,780
9/2020, $74,772,648
4/2021, $83,488,703
4/2018
5/2018
6/2018
7/2018
8/2018
9/2018
10/2018
11/2018
12/2018
1/2019
2/2019
3/2019
4/2019
5/2019
6/2019
7/2019
8/2019
9/2019
10/2019
11/2019
12/2019
1/2020
2/2020
3/2020
4/2020
5/2020
6/2020
7/2020
8/2020
9/2020
10/2020
11/2020
12/2020
1/2021
2/2021
3/2021
4/2021

Distribution of ARLIS Project Types



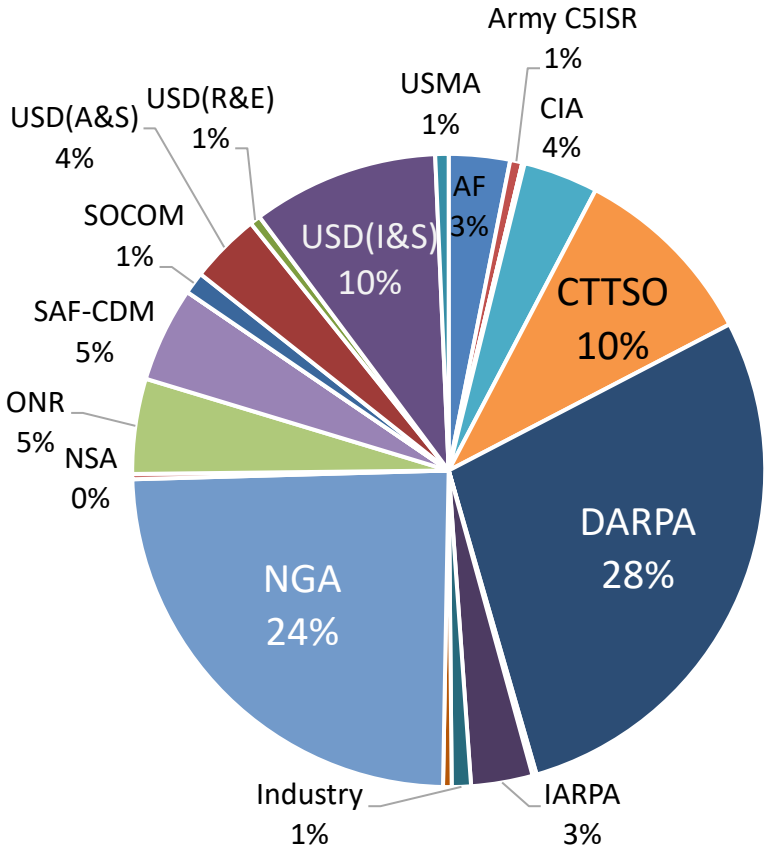


	FY 2018	FY 2019	FY 2020	FY 2021 estimate	Total
EXPENDITURES GRAND TOTAL	3,691,453	7,045,168	17,435,830	27,876,883	**56,049,335**

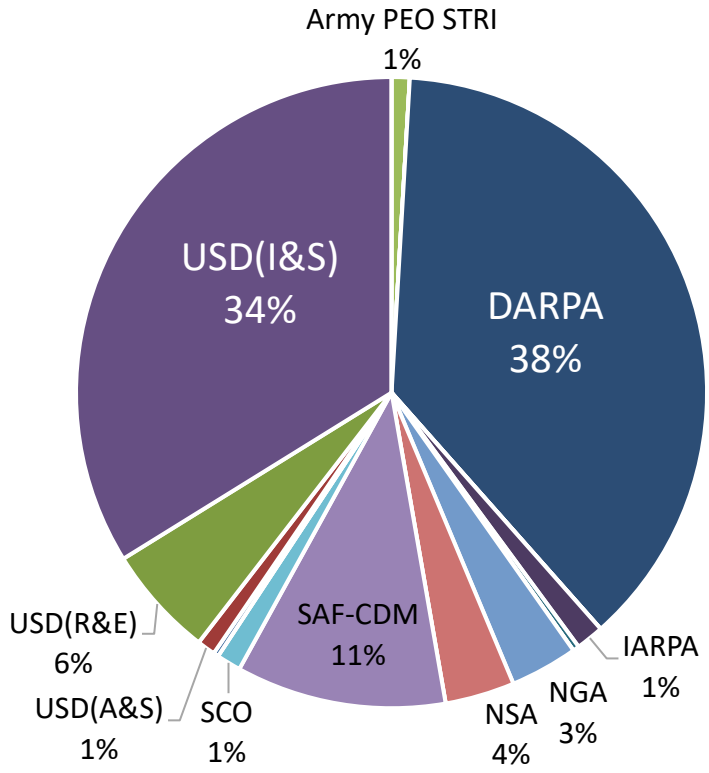
Expenditures as of 2/28/21: $17M.

Sponsorship Profile

USG FY19

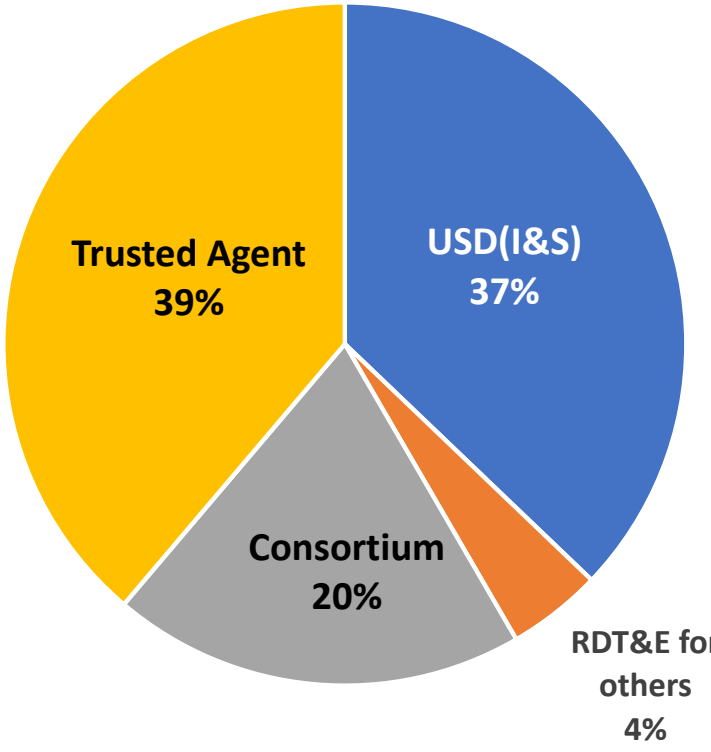


USG FY20

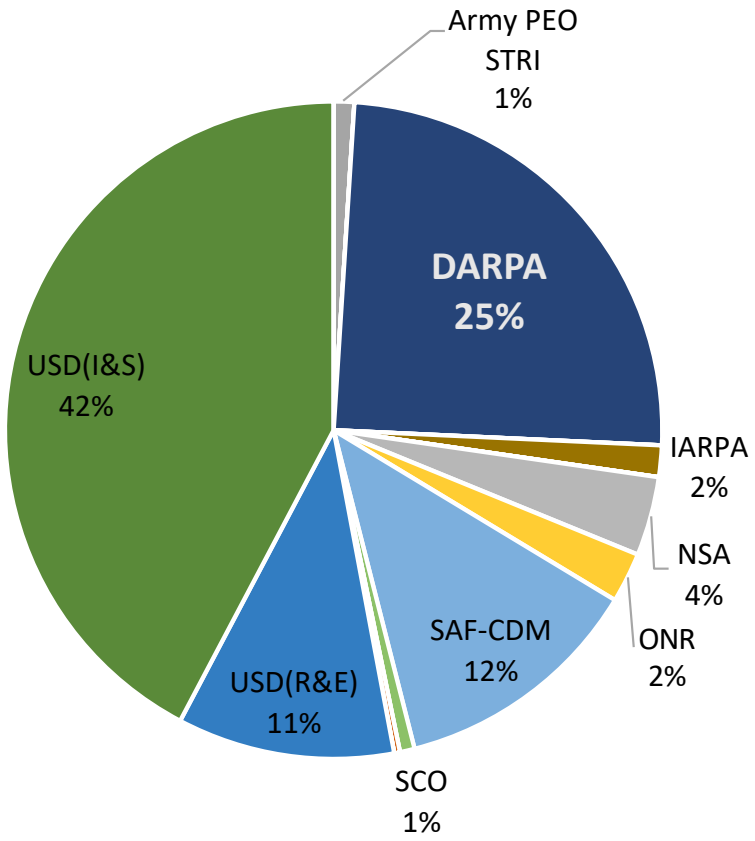


May 2020 – April 2021

Activity Profile, May20-Apr21



Sponsorship Profile, May20-Apr21



Program Portfolio for ARLIS

S&T/etc Domains	Mission Areas and Mission Drivers						
	T&E/V&V	**Operational & Mission Support**	**Influence & Narrative**	**Vetting, Insider Risk, CounterIntel**	**Technology Protection & Security**	**Training, Education & Aptitude**	**Tradecraft Support & S&T Expertise**
AAA / HCI / DataSci							
Social and Behavioral/ Language and Culture							
Policy, Law, Training, Education							
Cyber, CogSec, Infrastructure, Advanced HW (inc AR/VR etc)							

PROJECTS COME THIS WAY

S&T/etc Domains	Mission Areas and Mission Drivers						
	T&E/V&V	**Operational & Mission Support**	**Influence & Narrative**	**Vetting, Insider Risk, CounterIntel**	**Technology Protection & Security**	**Training, Education & Aptitude**	**Tradecraft Support & S&T Expertise**
AAA / HCI / DataSci							
Social and Behavioral/ Language and Culture							
Policy, Law, Training, Education							
Cyber, CogSec, Infrastructure, Advanced HW (inc AR/VR etc)							

S&T DISCRIMINATORS and CORE COMPETENCIES

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY
UNIVERSITY OF MARYLAND

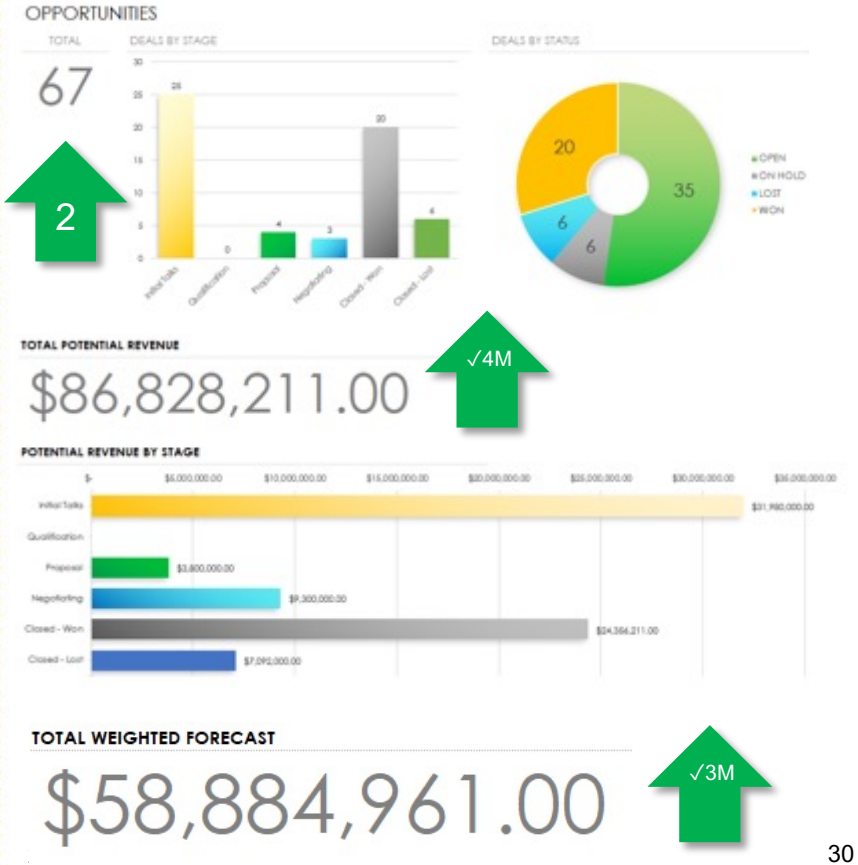
Where is ARLIS Today?

S&T/etc Domains	Mission Areas and Mission Drivers						
	T&E/V&V	Operational & Mission Support	Influence & Narrative	Vetting, Insider Risk, CounterIntel	Technology Protection & Security	Training, Education & Aptitude	Tradecraft Support & S&T Expertise
AAA / HCI / DataSci	✓✓✓✓	✓		✓	✓		✓
Social and Behavioral/ Language and Culture	✓✓✓	✓	✓✓✓✓	✓	✓		
Policy, Law, Training, Education	✓	✓			✓	✓	✓
Cyber, CogSec, Infrastructure, Advanced HW (inc AR/VR etc)	✓					✓	

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY
UNIVERSITY OF MARYLAND

ARLIS Program Development Pipeline

CRM Dashboard



ARLIS, as a "new" UARC, must stay focused on relationship building

- Agencies and organizations
- Their problems and topics
- Identify roles for ARLIS

Discoveries in the last 12 months

- A UARC is a new idea to the IC and security community
- ARLIS competencies and mission areas are not duplicative of other FFRDCs and UARCs

Thinking about ARLIS in 2021

- The University Affiliated Research Center with the core competencies to address the breadth of problems around **"all of society"** forms of conflict
- ARLIS at the center of both research AND operational activities for the nation in these critical areas
- Comport ourselves as a US Government laboratory operated by UMD
  - We are the nation's trusted agent first…
    the trusted agent for the human and information domain.
- Focus on **execution**
  - Must build specific tangible platforms; must embed with operational users
  - Must create research products; must establish testbeds and facilities
- ARLIS activities (group/individual) must lead to
  - Tangible scientific, research, or technical outcomes
  - Specific sponsored programs or projects or transition

ARLIS: Priorities for 2021

- Establish the ARLIS UARC as an OUSD(IS) resource and serving the Defense Intelligence & Security Community (NGA, DCSA, DIA, NSA, NRO)
- ARLIS Themes for 2021-2022:
  - Program Execution, Excellence, and Impact
  - Operational engagement: supporting the warfighter, intelligence analyst, and security personnel; (SOCOM, PEO STRI, TISMO, CyberCom)
  - Sensemaking from Publicly Available Information (PAI) and support for OSINT
  - "Risk/Trust": From individuals to supply chains, rethinking how we manage trust
  - Information as operational environment and **Cognitive Security Proving Ground** as unifying concept for winning operations in the information environment
  - AAA supporting cross-cutting activities (OUSD(IS), NGA, DNI, DIA…)
  - Continued focus on people, talent pipeline, training, education

ARLIS: Priorities for 2021 (cont.)

- HLT Mission Area (Michelle and Victor)
- New University-ARLIS business model and financial structure
  - Administrative transformation, scale and quality of service
  - Post-award support, contracting agility, procurement, human capital
  - Processes and people: one team, shared processes, distinct roles
- Expand INSURE Consortia activities
- Industry engagement

ARLIS: Enabling the Intelligence Edge

- OUSD(IS) is the strategic sponsor for ARLIS, providing the DoD (and IC) with a new UARC to specifically support **the Intelligence & Security mission**
- Provides the community with a new **independent and trusted** capability for applied research, operational support, and TE&VV (TRL 3 thru TRL 7+) in ARLIS competencies**: (1) Social Science; (2) AI/Autonomy; (3) Info Tech**
- ARLIS is **the only UARC with social science, human behavior and culture as core competencies**. ARLIS provides OUSD(IS) a mechanism and facility for
  - For leveraging and harnessing S&T activities in ARLIS's core competencies across all relevant DoD and IC agencies for I&S program needs
  - Exercising national and global sci/tech/policy leadership in OUSD(IS) mission areas and in the areas of ARLIS core competency
  - Access to a network of universities (**INSURE**) to conduct applied and restricted research to support Intelligence and Security missions; six member institutions, support from DDR&E HBCU program office, …

William Regli

Executive Director

Applied Research Laboratory for Intelligence & Security

Professor of Computer Science

The University of Maryland at College Park

regli@umd.edu

Cognitive Security & Operations in the Information Environment

Mission Area Session

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Cognitive Security & Operations in the Information Environment

Michael Bunting, Ph.D., Director for CSIOE

mbunting@arlis.umd.edu; mbunting@umd.edu

DoD & IC Prioritize Strengthening U.S. Cognitive Security & Operations in the Information Environment (CS/OIE)

Three troubling trends:

1. Growing number of threat actors (state, non-state, hacktivists & leaktivists) targeting the U.S.
2. With increasingly sophisticated intelligence capabilities and technologies at their disposal (e.g., cyber tools, biometric devices & big data analytics)
3. Using enhanced capabilities against traditional national security targets –*and*– other federal agencies, private sector, academe & public opinion

Source: U.S. National Counterintelligence Strategy, 2020-2022

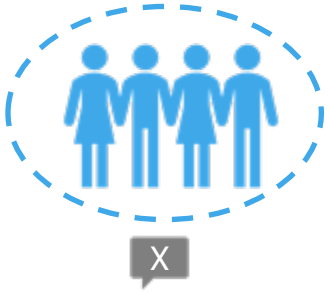
Cognitive Security

Meeting the challenge of this growing problem

Malicious influencer

Cognitive Security

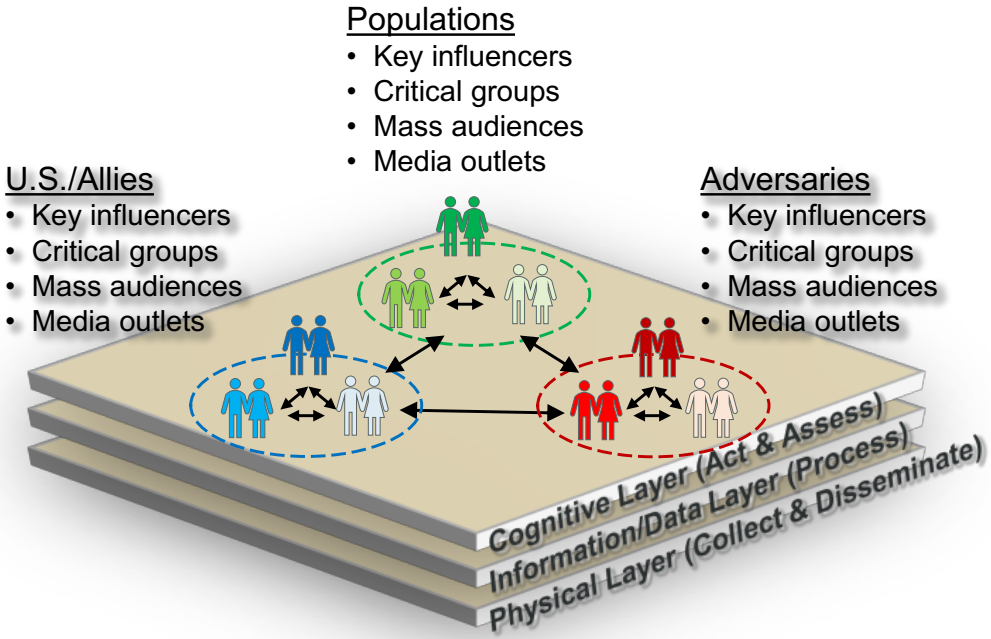
Resilient population



Susceptible population

Ineffective influencer

Operations in the Information Environment



On-/off-line Information Environment
(within context of larger multi-dimensional operational space)

Information environment: Aggregate of individuals, organizations & systems that collect, process, disseminate, or act on **information**

Operations in the information environment: Actions for affecting perceptions, attitudes & other drivers of relevant actor **behavior**

Drawing on ARLIS's Strengths

Cognitive Security is an interdisciplinary problem demanding interdisciplinary and interorganizational solutions

- Calls for cleared ARLIS personnel in social & behavioral science, cultural analytics, modelling/simulation, AI/ML, and OIE
- Draws from the deep bench of interdisciplinary thought leaders at UMD & INSURE
- Forges relationships with other UARCs, FFRDCs and R&D organizations

Cognitive Security solutions require data

- ARLIS owns or has access to a wide range of relevant data (e.g., DARPA; IARPA; DOD; START ICONS, GTDB; global & regional transportation)

Meet the Cognitive Security Team

ARLIS Leads: Dr. Mike Bunting (PI), LTG (ret) Ed Cardon, Dr. Ruthanna Gordon, Dr. Brian Pierce & Mr. Matt Venhaus

Operational Expertise
- LTG (ret) Darsie Rogers
- Mr. Austin Branch
- Mr. Paul Cobaugh
- Mr. Joe Kelly
- Ms. Amanda Towler

Wargaming
- Mr. Devin Ellis
- Dr. Barnett Koven

Legal
- Mr. Harvey Rishikof

Cognitive, Operational & Social Psychology
- Dr. Breana Carter
- Dr. Kelly Jones
- Dr. David Martinez
- Dr. Susannah Paletz
- Dr. Judy Philipson
- Dr. Amanda Woodward

Engineering & Designers
- Dr. Susan Campbell
- Ms. Victoria Chang
- Mr. Jarrett Lee
- Mr. John Romano

Machine Learning/NLP
- Dr. Michael Maxwell
- Dr. Laurel Miller-Sims
- Ms. Valerie Novak
- Dr. Anton Rytting

Data Science & Statistics
- Ms. Meredith Hughes
- Mr. James Hull
- Ms. Bernadette Jerome
- Dr. Noah Silbert

Rhetoric
- Dr. Angie Mallory

Culture/Language Expertise
- Dr. Victor Frank
- Dr. Ewa Golonka
- Dr. Brook Hefright
- Ms. Marilyn Maines
- Dr. Michelle Morrison
- Dr. Adam Russell

Academic Partners:
- UMD Center for Geospatial Information Science (Dr. Kathleen Stewart)
- UMD Language Science Center (Dr. Tess Wood)
- University of Melbourne Hunt Lab (Dr. Tim Van Gelder)
- University of Buffalo (Dr. Dave Doermann)
- Institute for Human Machine Cognition (Dr. Bonnie Dorr, Adam Dalton, Brodie Mather)

Information Propagation Fundamentals

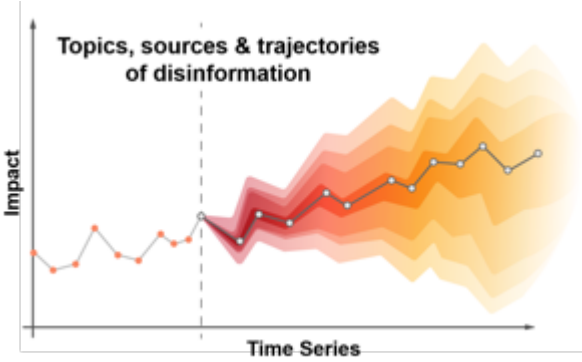
How do messages propagate, go viral, stay sticky, have impact?

You will hear about

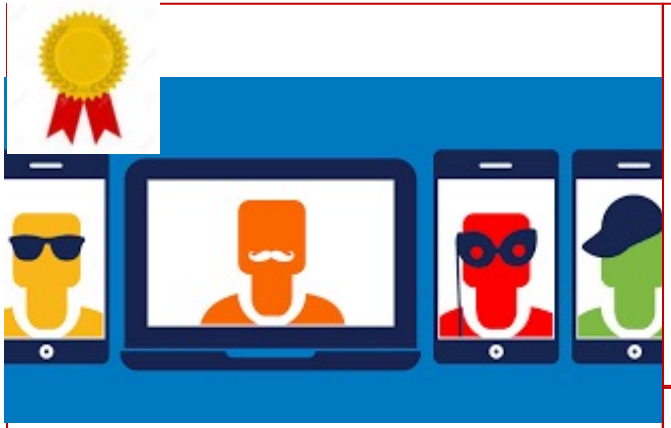
Capturing Emotional Expression in Social Media

Incubating

Social Weather Forecasting of High-Potency Stories



Personas & Scenarios



- Persona creation & detection
- Plausible online scenarios
- Real ID of online actors

You will hear about

Computational Social Science: Personality & Cognitive Ability Classification

Languaculture Virtual Assistant for Strategic Communications (LVASC)

Incubating

Computational Psychology: Modeling the True Self

CS/OIE Themes

Societal Cognitive Defense

- Reduce vulnerability to malinformation & manipulation
- Detect and mitigate
- Inoculate populations against malign influence

You will hear about

Dark VR: Virtually False Memories & Dark Uses of Virtual Reality

Stance detection (collaboration with IHMC)

Incubating

Training: HUMINT Recruitment & Exploitation

Cyber Wargaming

CS/OIE Themes

Data Sets & Data Analytics

- Curating social media data
- Maintaining low & high-side data repositories
- Building routines for sanitization & anonymization
- Navigating IRB, legal & ethical issues on public use & informed consent

You will hear about

DARPA Influence Campaign Awareness & Sensemaking (INCAS)

China Belt & Road: A Multilingual Analysis of Influence in Africa

Incubating

Acquire the PanTera Suite of Tools for On-line Information Operations

Big Wins

- New Project: *T&E support to DARPA Influence Campaign Awareness and Sensemaking (INCAS),* PI: Amanda Towler & Devin Ellis
- Resurrected the Phoenix Challenge conference, convening 200 cognitive security leaders to share needs and capabilities
- New Project: *OUSD(I&S) Sociotechnical Analyses of International COVID Information Environment*, building on Dr. Ruthanna Gordon's IRAD
- Member of these ODNI teams:
  - DNI Foreign Language Executive Committee
  - IC Training Council
  - DNI HLT Technical Experts Group

Cognitive Security Proving Ground (CSPG)

A Live, Virtual & Constructive modeling and simulation environment

Activities

- Research
- Engineering
- Test & Evaluation
- Wargaming
- Training

Current path

ARLIS Cognitive Security Proving Ground

Attempt to overcome challenges in the real world, or "in the wild"

Reduce risk on overcoming challenges before use in the real world

Experiments/ simulations/ test and evaluation in a secure, controlled environment

Groups of real people

Several real people and many bots (future)

Large numbers of bots (future)

Establish Capabilities for the CSPG (Task 1)

The **Cognitive Security Proving Ground** will meet IC & DOD needs for applied research and development in the information environment:

- Leverage ARLIS's deep bench of operational subject matter expertise and its roles as convener, innovator, and thought leader
- Provide timely, accurate insight, evaluation, and planning capabilities

Establish Capabilities for the CSPG (Task 1)

Goals

1. Define operational requirements & design for the CSPG, deliver in CONOPS form
2. Use information-gathering process as relationship-builder with customers
3. Unite ARLIS mission areas around shared tech requirements

New Research Methods (Task 2)

Goal: Increase complexity, scale & speed of applied research to better meet customer requirements

Completed: Literature review
- IDed cutting-edge methods relevant to Cognitive Security
- BRI use case provides basis for example CSPG research
- Described initial concepts for new live/virtual/constructive methods

Completed: SME consultation
- Small-group discussions to enhance and expand applied research concepts
- Outcome: pilot research protocol(s) and white paper seeds

Current Activity: Prototype new methods
- Based on key use cases (e.g., Belt and Road Initiative), carry out pilot study and capture lessons for effective research to support customer requirements
- Outcome: Report on method effectiveness and required capabilities for expansion

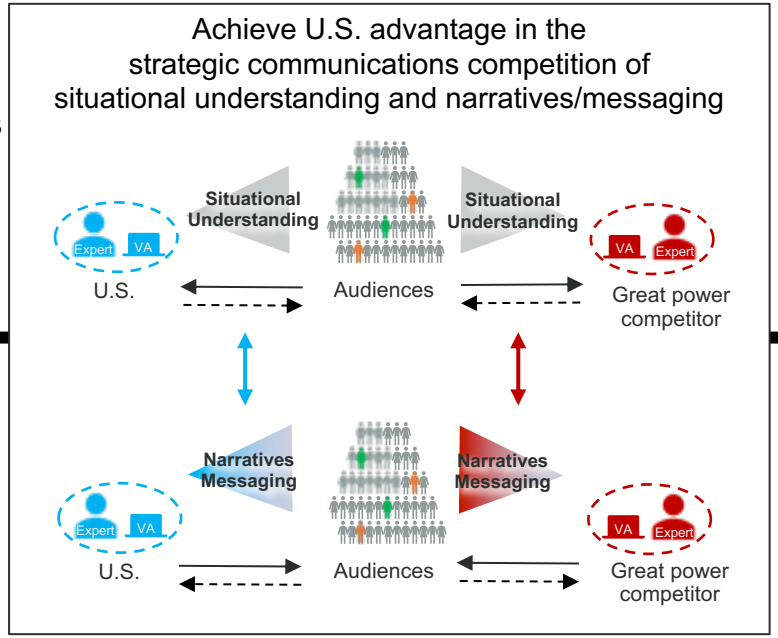
Languaculture Virtual Assistant for Strategic Communications (Tasks 3 & 4)

Amplify U.S. influence in great power competition via enhancement of strategic communications using an AI-based virtual assistant

Today

Strategic Communications

- Largely manual, with bulk of work performed by human strategic communications expert
- Long timelines to acquire knowledge for situational understanding, and to plan and execute narratives/ messaging - in competition with adversaries



= Human Expert + Virtual Assistant (VA) Team
Blue = U.S. and Red = Great power competitor

Future

Strategic Communications

- Virtual Assistant partners with human strategic communications expert to accomplish more in less time
- Shorter timelines to acquire knowledge for situational understanding, and to plan and execute narratives/messaging - in competition with adversaries

Languaculture Virtual Assistant for Strategic Communications (Tasks 3 & 4)

Aim: Take the first steps in the development of a virtual assistant helping a human expert in strategic communications.

Building upon AI-based agent technology developed by the Institute for Human & Machine Cognition (IHMC), the first steps are these tasks:

- **Situational understanding** - Assist in the automated extraction of a set of stances (beliefs about an issue, e.g., China's Belt and Road Initiative, and the strengths of these beliefs) expressed in social media (Twitter for the project) at the individual and group level.
- **Narratives/messaging** - Assist in planning and executing narratives/messaging with suggestions of possible campaign courses of action based upon a number of elements that include stances, audiences, key influencers, cultural norms, and influence tactics.

Multi-disciplinary team
Team synergizes ARLIS's deep expertise in social/behavioral sciences and strategic communications with IHMC's extensive skills and knowledge in AI-based, virtual assistant and bot technologies.

Phoenix Challenge Conference (Task 5)

ARLIS and the Information Professionals Association revived the Phoenix Challenge Conference Series with support from OSD, JS, AF

Date: April 13, 2021 – UNCLASSIFIED – Online

- Coordinated with USCENTCOM's Worldwide Information Operations (IO) Conference April 14-15, 2021.

Convened: 200 Senior USG, Allies, & Industry as active participants, invitation only

- Keynote: Former Under Secretary of Defense for Intelligence Dr. Michael Vickers
- Panel 1: Information Effects in Strategic Competition – Managing Peer Competition and Current Operations in a Hyperconnected World
- Panel 2: Risk Based Models for Acquisition Security & Insider Threats in the Modern Information Environment
- Panel 3: Commercial Technology Trends and Effects on OIE – New Tools & New Risks
- Plenary panel: Creating an Interconnected Platform for Testing, Evaluation, Simulation, Training, Exercise & Mission Rehearsal to support OIE

China Belt & Road Initiative: A Multilingual Analysis of Influence Evidence in Africa (Task 6)

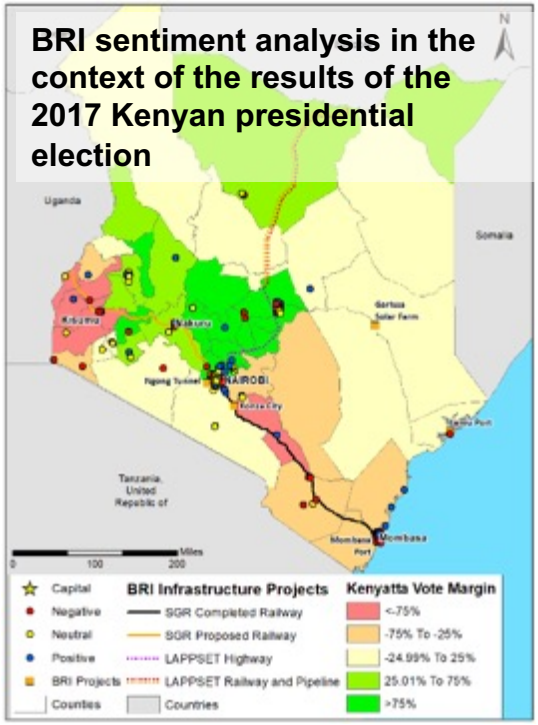
Research Questions:

- What are the **attitudes and sentiments of Kenyans** towards domestic Kenya-China BRI projects?
- Are **indicators of Chinese influence** revealed through automatic and manual text analysis?

Why Kenya? Key entry point for Chinese influence in East Africa through BRI investment projects.

Preliminary Results: Social media analysis reveals attitudes re:

- Kenyan debt
- Chinese loans & investments
- Socio-cultural messaging with references to colonialism, Chinese influence, and cultural differences
- Kenyans' attitudes expressed toward China and BRI infrastructure



China Belt & Road Initiative: A Multilingual Analysis of Influence Evidence in Africa (Task 6)

Research Approach:

- Integration and analysis of disparate data sources
- Multilingual social media dataset focused on China and BRI topics (in English and Swahili)
- Combination of automated methods of analysis (e.g., topic modeling, sentiment analysis) with manual analysis
- Spatial pattern analysis of geocoded social media data as well as demographic and other georeferenced datasets
- Development of ontology of state and institutional actors
- Exploration of other Kenyan media sources for influence parameters

Team: Dr. Michelle Morrison (ARLIS, PI); Dr. Kathleen Stewart (Professor & Director, UMD Center for Geospatial Information Science), Dr. Tess Wood (UMD Language Science Center)

CS/OIE Project Constellation

Applied Research & Engineering

Innovative Research Methods

Influence Shapes the Pandemic

China BRI Geolinguistic Mapping

Linguacultural Virtual Assistant

Cross-Cultural Emotion Annotation

Inferred Psychological Attributes

Test & Evaluation

DARPA INCAS

DARPA Vienna

Gold-Standard Data Curation & Annotation

- BETTER
- MATERIAL
- BABEL
- DARPA KAIROS
- NSA

Wargaming & Operational Focus

Cyber Wargaming

China Working Group

Russia Working Group

Africa Working Group

Transition & Training

HUMINT Training

Phoenix Challenge Workshop

Current

PEO STRI

USASOC

USD(A&S)

USD(I&S)

DARPA

IARPA

Intelligence Community

CS/OIE Operational Customer Focus

DIA

SOCOM

CYBERCOM

J8 & J39

Global Engagement Center

SCO

SAF/CDM

Program Development

Thank you!

Michael Bunting, Ph.D.
Director for Cognitive Security & Operations in the Information Environment
(301) 226-8894
mbunting@umd.edu
mbunting@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Task Order – further details in backup slides

Cognitive Security Proving Ground (CSPG)

- **Sponsor:** OUSD(I&S)
- **Program Manager/Client:** Amanda McGlone, OUSD(I&S) amanda.r.mcglone.civ@mail.mil
- **Period of Performance:** 05/19/2020 – 09/30/2021
- **TRL of the work:** 4 – 5
- **Total Budget:** $3,081,898
- **Expenditures:** $1,321,887 as of January 2021

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Computational Social Science

Anton Rytting, Associate Research Scientist
crytting@arlis.umd.edu

Computational Social Science

- Sponsor: ODNI
- Program Manager/Client: ODNI
- Period of Performance: 18Aug19—31Dec20
- TRL of the work: Going from 4 to 5
- Total Budget (+ Expenditures to Date): $1,181,706

Team Members

- **PI** Mike Bunting; NCE: **PI** Anton Rytting & **Co-PI** Victor Frank
- Valerie Novak, James Hull, Paul Rodrigues, Ewa Golonka, Jarrett Lee, Laurel Miller-Sims, Tom Conners, Michelle Morrison, Aric Bills
- *UMD Students:* Xiuwei Li (INST), Ali Bhatti (INST), Kevin Ngo (INST), Samara Orellana (INST), Dhanvee Ivaturi (CS), Daniel Smolyak (CS), Adam Factor* (Psychology)
- *Consultants:* Susannah Paletz, Petra Bradley

Project Description *[1 of 3]*

Goal: *Ascertain a person's personality traits (including Big 5 and Dark Triad) from his/her electronic text (e.g., blogs, social media posts)*

SWOT: Current Approaches:

- ~10 years research using supervised machine learning (e.g., Golbeck et al. 2011), but very little use of DNNs
- Limited work in non-English languages, non-public social media
- No prior work combining personality traits with cognitive factors

Project Description *[2 of 3]*

Outcomes:

- Corpus: Anonymized dataset of VK, LiveJournal, Twitter and Blogger from 1293 participants (over 917K posts, 49M words total)
- Russian Feature Extraction Toolkit (RFET):
  - NLP toolkit with 65+ features used as input for ML systems.
  - Includes varieties of laughter, grammatical information, and features referenced in Personality/Psychology literature
- Methodology/pipeline applicable to other languages, platforms

Project Description *[3 of 3]*

Intrinsic success measures:

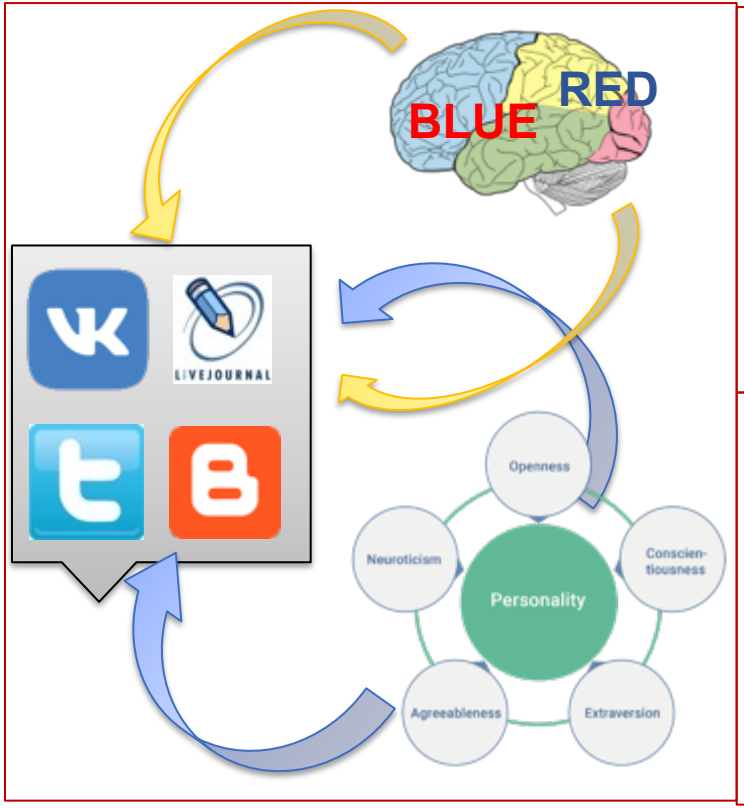
- Corpus: size of collection (number of participants, posts, words)
- RFET: accuracy (RSME) of inference of personality traits from text.

Extrinsic success measures:

- Extension of methodology to other languages, genres, situations
- Successful indication of sudden changes to personality traits.

Expected Impact: *USG's insights into a foreign contact's personality in a relevant language without face-to-face contact.*

CSS Overview



Objective: Automate inference of personality and cognitive profiles from social media text

Project completed.

Deliverables: Ground-truth corpus of text + profiles, Language-specific features for machine learning (RFET)

Relationship to ARLIS's goals/story

- Understanding how personality traits are reflected in text is critical to "the people side" of NLP and the sociotechnical realm
- The CSS project's findings and methods are potentially relevant for Countering Insider Risk (e.g., Task 3) and Languaculture Virtual Assistant for Strategic Communications (LVASC). The corpus could be relevant for the Cognitive Security Proving Ground (CGPG).
- ARLIS has been well-positioned as a UARC to conduct corpus collection perhaps not possible for other entities.

Big Wins (so far)

- Key insights, what's the "wow"?
  - Likely the world's largest collection of VK data associated with cognitive traits—almost certainly the largest collection of any trait-tagged text readily available to USG & U.S. researchers for this language
  - Construction of pseudonymization pipeline to protect participants' privacy while maintaining natural text for downstream experiments
- Important papers
  - Manuscripts on RFET, corpus to be submitted to RANLP or similar venues
- Transition, users, etc.
  - Database made available to the Cognitive Security Proving Ground

Next Steps and Future Capabilities

- Activities and milestones ahead
  - Refinements of automatic anonymization underway, to create natural sounding pseudonymized/anonymized text.
  - IP disclosures for RFET and anonymization process for UMD Office of Technology Commercialization
- Transition goals/obstacles
  - Corpus to be used by the CSPG
- New ideas and whitepapers
  - Brook Hefright's white paper on Great Power Competition for DIA
- Sponsor relationship, new/additional sponsors
  - Mike Bunting has been in touch with sponsors with similar needs

Thank you!

Anton Rytting

crytting@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Minerva Project: The Role of Emotions in Adversarial Information Campaigns

Susannah Paletz, Research Professor, School of Information Studies

paletz@umd.edu

The Role of Emotions in Adversarial Information Campaigns

- **Sponsor:** Minerva Research Initiative/Office of Naval Research (ONR)
- **Program Manager/Client**: Dr. Rebecca Goolsby, ONR Program Manager
- **Period of Performance**: Feb. 18/June 18, 2019-May 17/Aug. 22, 2022
- **TRL of the work**: Basic research, funding type 6.1
- **Total Budget**: $1,499,997; $812,579 spent so far
- **Team Members**:
  - **PI:** Dr. Susannah Paletz, UMD College of Information Studies
  - **ARLIS**: co-PI Dr. C. Anton Rytting, Dr. Ewa Golonka, Mr. Nick Pandža, Ms. Nataliya Stepanova; Mr. Bret Howard, Ms. Nabeela Alam, Mr. Rick Phillips
  - **UMD ICONS/START**: Ms. Egle Murauskaite, Mr. Devin Ellis
  - **New Jersey Institute of Technology**: Dr. Cody Buntain
  - 9 research assistants at University of Wrocław, Poland and 3 in Vilnius, Lithuania; gratitude to Dr. Alicja Keplinger

Project Description

Goal: Understand the impact of different emotions on social media sharing/engagement; interrelationships between different other factors and emotions.

SWOT of current approaches:

- Strengths: sophisticated computational work; advances in psychology of emotions
- Weaknesses: these areas rarely inform each other; focus on text
- Opportunities: multidisciplinarity will bring greater rigor, novelty
- Threats: multidisciplinary work difficult to conduct, publish

Project Description

Expected Outcome: better understanding of role of emotions in combination, emotional complexity, in social media sharing; emotional content of different topics, media, etc.

Success measures:

- Quality measures:
  - Size of corpora
  - Intercoder reliability standards
  - Ability to control for covariates
- Impact measures:
  - Presentations, publications; eventually, citations
  - Others utilizing our annotation scheme
  - Co-developing methods for scaling up annotation
  - Possibility of translation of research to USA/NATO groups

Project Description

Expected Impact:

- Advance computational social science of emotions
- Understand role of emotions in social media sharing beyond current practice
- Progress in multimodal social media research

Emotions in Social Media Overview

Activities and Objectives	Status
Identify Polish and Lithuanian sociopolitical influencers	complete
Collect and sample social media data, links, metadata (YouTube, FB, etc.)	complete
Annotate for emotions in native language	complete
Other annotation (topics, media, language)	on sched
Statistically analyze (emotional profiles, effects of emotions on sharing, etc.)	on sched
Computational linguistic analyses of corpus	on sched
Present, publish findings	on sched

Polish Example

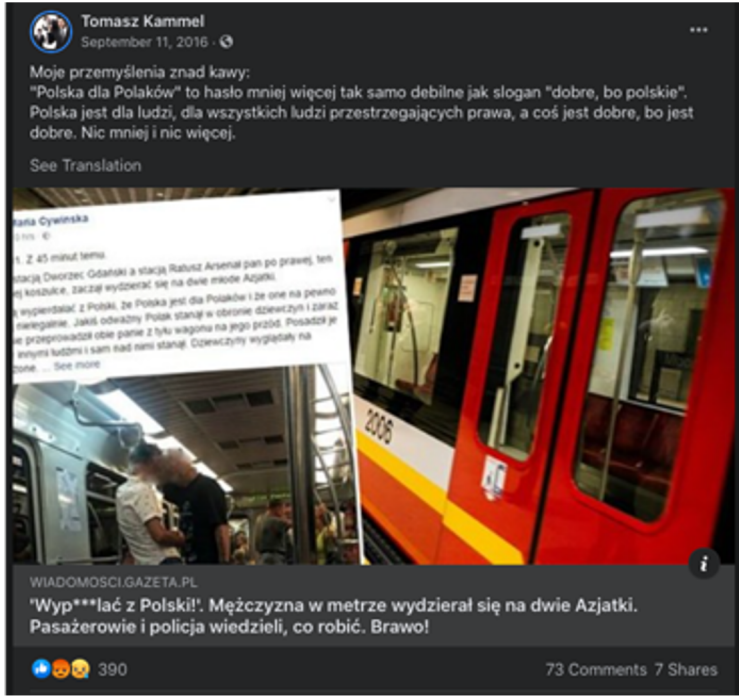
Translation

My thoughts over coffee: "Poland for Poles" is a slogan more or less as dumb as the slogan "good because it's Polish". Poland is for people, for all law-abiding people, and something is good because it is good. Nothing less and nothing more.

Text on the bottom: 'Get the f**k out of Poland!' A man on the subway yelled at two Asian women. Passengers and police knew what to do. Bravo!

Emotion Annotation

Anger: 50	Hate: 20
Contempt: 30	Admiration: 43
Pride: 5	Sadness: 10
Fear: 4	Excitement: 18



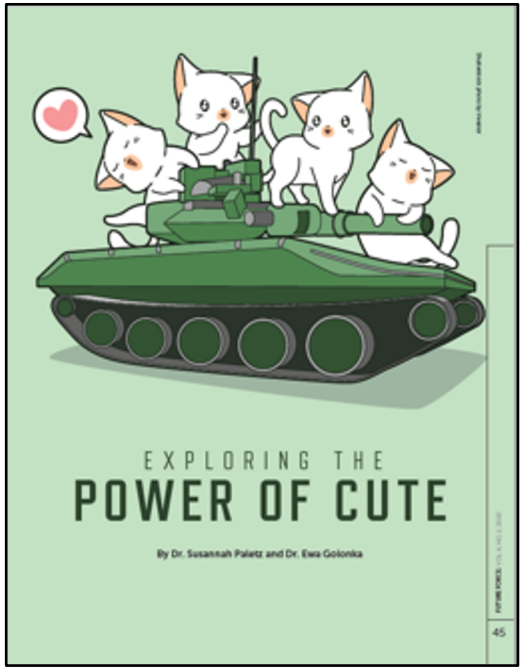
Relationship to ARLIS's goals/story

"Understanding how emotion and affect function and influence people's thoughts, beliefs, and actions therefore has clear utility for intelligence analysis; drawing on foundational and emerging work in this area...is a key frontier for SBS researchers and the IC." (National Academy of Science, 2019, p. 92. *A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis*)

- Emotions are fundamental to the human domain.
- This work ties to ARLIS projects on narratives, social media annotation, influence, cognitive security.
- Leverages ARLIS and START scientific expertise, UMD faculty, international partners.

This project succeeds because of a multidisciplinary, multinational collaborative team delving into mission-relevant cutting-edge science.

Big Wins



- Emotion annotation guide shared with 28 interested parties, including Air Force Research Laboratory PM, Wil Corvey (DARPA)
- Precursor work described in *Future Force* (2020)
- Emotion annotation method featured in a UMD Social Data Science (SoDa) presentation/panel (Paletz, Nov. 2020)
- Some emotions from codebook being used in project on incels at Smart Information Flow Technologies (SIFT; Sonja Schmer-Galunder)

Big Wins

- Ms. Stepanova to be Marshall scholar at U of Edinburgh (Fall 2021)
- Ms. Stepanova, with Dr. Rytting, led poster presentation (MIRS 2021) with computational linguistic Polish Facebook (FB) findings:
  - Author popularity more predictive than topic: FB engagement on authors' other posts predicted shares on target posts
  - Some topics predicted sharing of FB posts: vaccination of children
- Overall project informing DARPA program(s), Air Force Research Laboratory PM

Project Status Wins: Data Collection

Social Media	Poland 🇵🇱	Lithuania 🇱🇹
Sociopolitical entities identified	365	188
Facebook (FB) accounts, *posts* scraped	328 *2,246K*	142 *551K*
YouTube (YT) channels, *videos* scraped	170 *333K*	84 *192K*
Sampling: 2 elections, COVID lockdown #1, major non-election events	women's strike	Baltic liberal party scandal

Project Status Wins: Data Annotation

Posts Annotated	PL 🇵🇱	LT 🇱🇹
Emotion: FB	3,732	2,039
Emotion: YT	731	417
Media: FB	3,659	1,740

In process annotation

- Topic (adapted Comparative Agendas Project master codebook)
- Language(s)

Annotation is on the entire post.

Summary Emotions Reliability (Facebook) (coded separately, used ICC) Polish (PL, 3 groups) and Lithuanian (LT)
≥ .90 for Gratitude (PL, LT); Happiness (LT); Kama muta (LT); Sexual attraction (LT)
≥ .85 for Anger (PL); Amusement (PL, LT); Love (PL, LT); Gratitude (PL); Sadness (PL); Wonder (LT)
≥ .80 for Admiration (LT, PL); Contempt (PL, LT); Happiness (PL); Pride (PL, LT); Sadness (LT)
≥ .75 for Confusion (PL, 2 groups); Embarrassment (PL, LT); Excitement (PL); Fear (PL, LT); Hate (PL); Kama muta (PL, though two groups >.85); Sexual attraction (PL); Surprise (LT)
≥ .70 for Anger (LT); Disgust (LT); Empathic Pain (PL, LT); Surprise (PL); Wonder (PL)
Rare or very rare, poor reliability: Confusion (PL, LT), Disgust (PL), Excitement (LT) Embarrassment (1 PL group), Envy, Hate (LT), Nostalgia (varies), Relief

Project Status Wins: Behind the Scenes

- Emotion codebook adapted for 2 languages/cultures
- 20+ months of annotation so far: 4 teams, 2 countries
- Data munging across multiple annotation sets; documentation, version control
- Computational linguistic analyses of topics, account-level engagement
- How to measure narratives?
  - Topic modeling
  - Topic annotation (CAP codebook adapted for our project)
  - Catchphrases, election slogans, mentioning Russia (present/absent)
  - Similarity analyses of FB posts with narrative discussions (attempted proof-of-concept)
- Planned sophisticated statistical analyses of multilevel, non-parametric data
  - Emotional profiles for Lithuanian posts mentioning Russia vs. not
  - Emotional profiles of different catchphrases, topics, etc.
  - Patterns of emotions associated with sharing, likes, etc.
- Created website: https://emotionsinsocialmedia.umd.edu/ (Mr. Phillips)

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Emotion annotation guide translation/adaptation	June-Oct. 2019	Complete
Recruitment, hiring, training of annotators	Mar.-Nov. 2019, ongoing	Complete/ on sched
Identification of sociopolitical influencers, accounts, events	Feb. 2019-Oct. 2019	Complete
Social media data collection	June-Dec. 2019, March-Aug. 2020	Complete
Annotation	Sept. 2019-Aug. 2021	on sched
Data preparation	Dec. 2020-Sept. 2021	on sched
Data analyses: statistical, computational linguistic, computational	Dec. 2020-June 2022	on sched
Writing up, submitting	Mar. 2021-Aug. 2022	on sched

Project Status: Risk Assessment

Risk	Mitigation
Technical: could not scrape all LT accounts	Lots of other data, acknowledge weakness
Technical: theory, measurement of narratives is contested, complex	Using different ways to measure and identify
Technical: annotation time consuming to do and lead	Increased % of excellent Golonka and Murauskaite
Technical: difficult to get good reliability for rare emotions	Acknowledged weakness - cannot train on what is not in corpus; suggests future work
Management: challenges in paying annotators, creating contracts in a timely manner	Multiple reminders sent to relevant UMD office helps; ARLIS processes working
Management: Minerva Research Initiative potentially cut	Y3 not cut
COVID-19: resulted in slowdowns, RA illness; no travel to train/iterate coding schemes	Teams already remote; team leads understanding; No Cost Extension; sampled Event 4

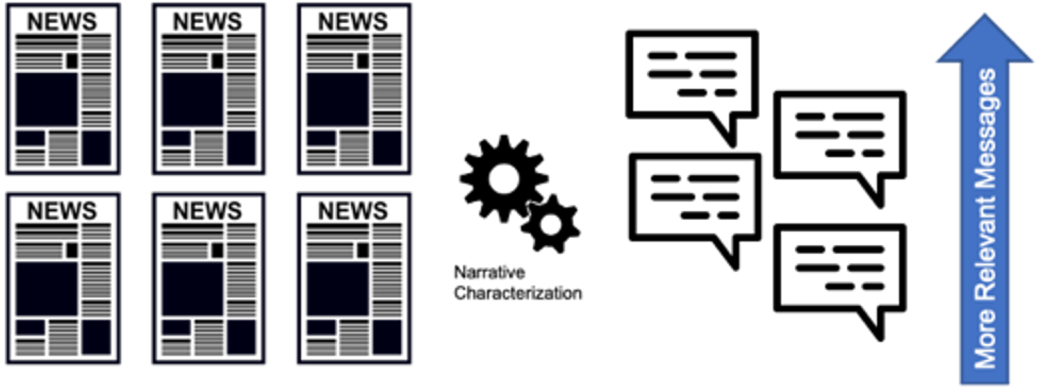
Next Steps and Future Capabilities

- Activities and milestones ahead
  - Finish annotation
  - Continue data management
  - Conduct many planned statistical analyses (brought on Mr. Pandža)
  - Carry out potential qualitative analyses
  - Conduct additional computational work on corpus
  - Submit papers

Potential Future Work (Buntain)

Information retrieval tools for identifying narrative-laden social media content

- It may be simpler to identify *journalistic* examples of a particular narrative
- Hypothesis: Ranking social media content by similarity to journalistic narrative examples will increase identified narrative content from social media



Next Steps and Future Capabilities

- Transition goals/obstacles
  - Conduct emotion annotation of corpora on US COVID Response project
  - Interest but no funding so far in creating larger English annotated dataset
  - Early stage potential opportunity for collaboration with MITRE D3I
  - Narrative collaboration initially disrupted, but Hefright, Rytting, Golonka will continue to explore in IRAD
- Sponsor relationship, new/additional sponsors
  - Regular contact with sponsor Dr. Goolsby
  - Successful Minerva Research Initiative review Oct. 29, 2020
  - DARPA's Computational Cultural Understanding Program

Thank you!

Susannah Paletz

paletz@umd.edu

College of Information Studies

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

https://emotionsinsocialmedia.umd.edu/

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Sociotechnical Analyses to Address the COVID-19 Pandemic

Ruthanna Gordon, Associate Research Scientist

rgordon@arlis.umd.edu

The Challenge of the "Infodemic"

Immunizing the public against misinformation

25 August 2020

World Health Organization

Soon after the world started getting used to the terms coronavirus and COVID-19, WHO coined another word: "infodemic" — an overabundance of information and the rapid spread of misleading or fabricated news, images, and videos. Like the virus, it is highly contagious and grows exponentially. It also complicates COVID-19 pandemic response efforts.

COVID Misinformation Is Killing People

SCIENTIFIC AMERICAN

INFODEMIC MONITOR

Bulletin of the Atomic Scientists

How Russia, China, and other governments use coronavirus disinformation to reshape geopolitics

By Isra Thange, Nicola Bariletto, Luca Zanotti, Jacob Rob, Samikshya Siwakoti, Jacob N. Shapiro, October 12, 2020

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

UNIVERSITY OF MARYLAND

What ARLIS Brings to Research on the COVID Information Environment

- **Behavioral and Social Science expertise:** Understand information spread in the context of cognitive and behavioral shifts
- **Linguistic and Cultural expertise:** Examine how narratives shift across communities
- **Social Media expertise:** Quantitative and qualitative analysis of the online messaging environment
- **Narrative expertise:** Understand how individual messages combine to create, and draw on the power of, larger ideas about COVID and the world

Relationship to ARLIS's goals/story

- Demonstrates use of multiple social science research methods in tandem
  - Major planned strength for the Cognitive Security Proving Ground
- Ties into other projects:
  - Mapping international IE (e.g., Belt and Road Initiative, Russia studies)
  - Annotating social media (e.g., Minerva)
  - Characterizing influence (e.g., INCAS)
- Acquiring data access and capabilities
  - International social media datasets

IRAD: Detecting and Tracking Malinformation During the COVID-19 Pandemic

- **Sponsor:** ARLIS IRAD
- **Program Manager/Client:** ARLIS
- **Period of Performance:** 4/12/20—10/11/20
- **TRL of the work:** Early applied research
- **Total Budget (+ Expenditures to Date):** $50,000
- **Team Members:**
  - PI: Ruthanna Gordon
  - Team: Kelly Jones, Michelle Morrison, Valerie Novak, Sarah Oates, Anton Rytting, Tess Wood

US COVID Response: Sociotechnical Analyses to Address the COVID-19 Pandemic

- **Sponsor:** OUSD(I&S)
- **Program Manager/Client:** Amanda McGlone
- **Period of Performance:** 12 months TBD
- **TRL of the work:** Analysis and proof of concept
- **Total Budget (+ Expenditures to Date):** $1.8M (pending)
- **Team Members:**
  - PIs: Ruthanna Gordon, Polly O'Rourke
  - Leads: Marilyn Maines, Kathleen Stewart, Susannah Paletz

Project Description

Goal:

- Track COVID narratives across international information environment (IE)
- Understand how COVID has shifted IE
- Test scientific principles for effective countermessaging
  - Focus on key anti-vaccination narratives in allied countries

Project Description

Current Methods SWOT:

- Considerable research on COVID disinformation
- Mostly in-country, mostly English
- Little on cross-border or cross-language spread beyond specific defined paths
- Little on long-term IE shifts

Project Description

Outcomes and Impact for USG:

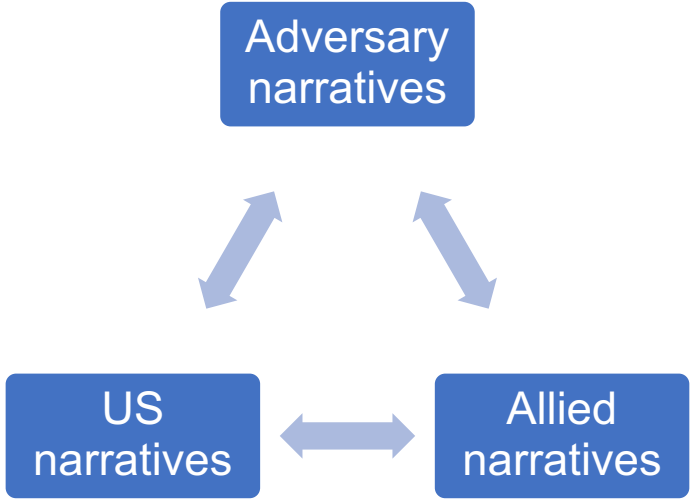
- Understand how COVID-19 affects U.S. global relationships
- Provide a foundation for potential mitigation strategies
- Increase preparedness for future outbreaks and pandemics
- Capture current COVID-19 international impacts

Success measures:

- Identifying continuity and changes in narratives across settings
- Actionable guidance for IO and public health

Overview

To understand the international IE, we need to track narratives everywhere



Understanding the IE lets us:

- Design and test responsive messaging
- Anticipate changing attitudes
- Anticipate future bio crises/conflicts

Deliverables focus on:

- Learning where narratives come from, who shifts them, where they go
- Messaging to support allied vaccination efforts
- Scanning for emerging tech

Big Wins (so far)

- Shifting the bar: Moving from descriptive data to actionable insight in large media datasets
  - IRAD creates a foundation for combining top-down and bottom-up strategies to characterize narrative patterns
- Insights and hypotheses from IRAD
  - Initial analysis suggests conspiracy theories and misinformation much more prevalent in English- than Spanish-language vaccine messaging (e.g., 5% mention of “Gates” vs. 0.21%)
  - Initial ID of Russian narratives denigrating Western vaccines in favor of Sputnik vaccines (e.g., “three queens”)

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
IRAD research	Complete	NCE
UCSR Kickoff	Awaiting contract	…
In-process review	Awaiting contract	…
Final Reports	Awaiting contract	…

- IRAD originally scheduled for 12 APR 2020 to 11 OCT 2020, extended due to data delays and business development needs
- Operation Warp Speed (now U.S. COVID Response) draft SOW received 5 FEB 2021
- SOW and Response sent 5 APR 2021
- Modifications requested 6 APR 2021 and provided 19 APR 2021

Project Status: Risks

Risk	Explanation	Mitigation Plan
Data access	• Zignal is gold standard, but gaps remain	• ID new sources to supplement core dataset • Seek location-specific sources
Research approval timelines	• Approval timelines affect ability to access and analyze data	• New approval process set • Milestones based on longer time frames
Timeliness of analysis	• IE changing rapidly with events • Analyses and research materials must remain relevant	• Plan for shifting analytic needs based on new developments • Focus on long-term IE changes

Next Steps and Future Capabilities

- Evaluate narrative tracking methods
  - Compare multiple direct response techniques (e.g., surveys, interviews) with social media to gauge how well each reflects population-level narrative patterns
- Measure and anticipate impacts that matter
  - Correlate social media analysis with multiple large datasets (e.g., CATT traffic dataset) to create better impact metrics
  - Use AI-augmented collective intelligence to connect online messaging with offline impacts in rapidly changing environments

Thank you!

Ruthanna Gordon
rgordon1@umd.edu
rgordon@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland
20742

www.arlis.umd.edu

ARLIS COVID leadership team

Polly O'Rourke (co-PI)
David Broniatowski (GWU)
Marilyn Maines
Michelle Morrison
Valerie Novak
Susannah Paletz
Valerie Reyna (Cornell)
Steve Sin
Kathleen Stewart
Rebekah Tromble (GWU)
Tess Wood

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Dark Uses of Immersive VR for Disinformation and Adversarial Manipulation

Ewa Golonka, Associate Research Scientist

egolonka@arlis.umd.edu

Dark Uses of Immersive VR

- **Sponsor:** ARLIS
- **Program Manager/Client:** ARLIS Leadership
- **Period of Performance:** 07/01/2020 – 30/06/2021
- **Total Budget:** $50K (Expenditures to Date $45,786)
- **TRL of the work:** 2 – 3
- **Team Members:** Ewa Golonka (PI), Victoria Chang, Victor Frank, Kelly Jones, Nick Pandža, Jacob Scocca

Project Description

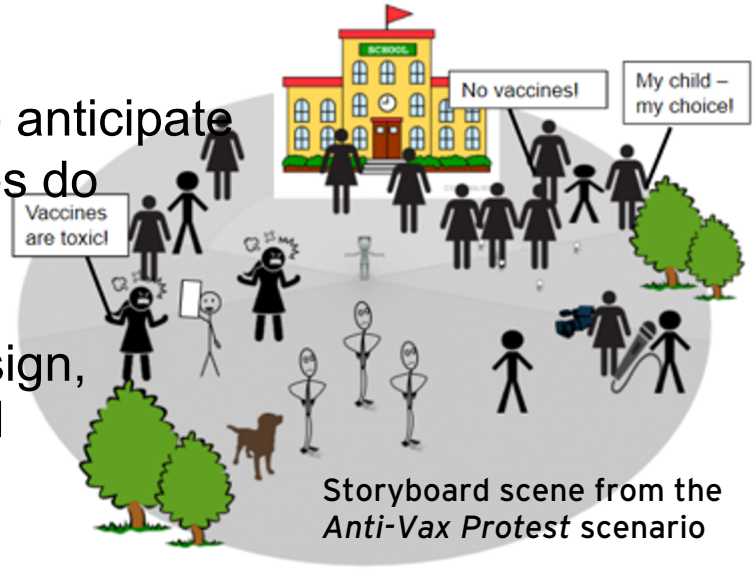
Strengthening the resilience of individuals against malicious influence in the information environment

Goal: Protect humans in information environment by understanding, identifying, and testing vulnerabilities of VR and VR users

Expected impact:

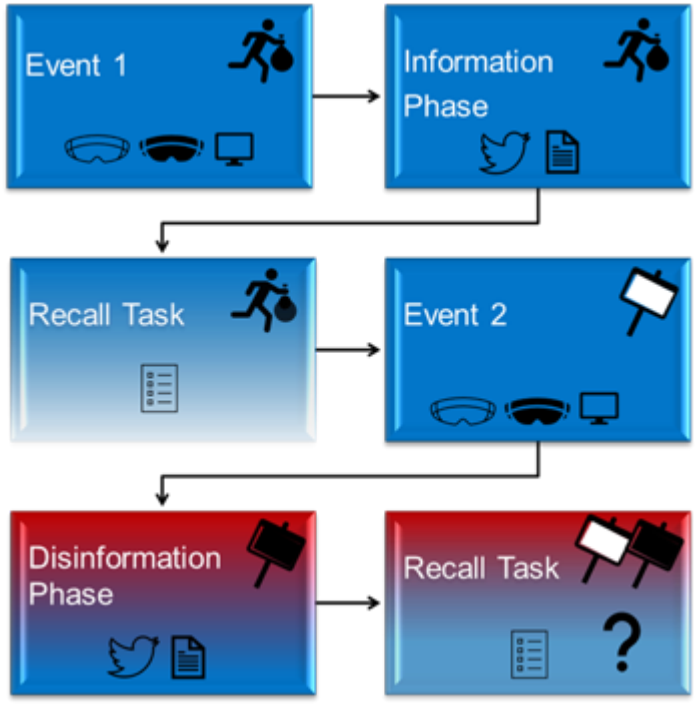
- Socio-technical research methods to anticipate strategic surprises before adversaries do
- Increase resilience of the population of VR users

Success measures: Rigorous study design, interest from potential clients, Registered Report published



Storyboard scene from the *Anti-Vax Protest* scenario

Dark Uses of Immersive VR Overview



Study design sketch

Project objective:

Develop research design to investigate effects of disinformation on creating false memories of VR experiences using social media as disinformation medium

Project status:

- Research design developed
- Registered Report written
- Seeking interested clients

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Technical Report *Virtually False Memories: The Misinformation Effect on Virtual Reality Experiences*	Completed	On schedule
Registered Report	In progress	On schedule

- **Big Wins**: Quality research design developed; understanding problem space: information environment, VR vulnerability, false memory
- **Transition goals/obstacles**: Secure funding for next phases
- **New ideas and whitepapers**: Exposure to disinformation in VR/AR environment or via deepfake technology; expand use cases
- **Sponsor relationship, new/additional sponsors**: Seeking contacts, prospective sponsors: DARPA, OUSD/R&E, JAIC, DOJ

Thank you!

Ewa Golonka
egolonka@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

INfluence Campaign Awareness and Sensemaking (INCAS)

Amanda Towler, Associate Research Engineer, atowler@arlis.umd.edu

Devin Ellis, Senior Research Scientist, ellisd@umd.edu

INCAS Program Testing &Evaluation

- **Sponsor:** DARPA
- **Program Manager/Client:** Dr. Brian Kettler
- **Period of Performance:** May 2021 – July 2025
- **Total Budget:** $6.5M (*no expenditures yet*)
- **TRL of the work:** going from 3 to 6
- **Team Members:**
  - PI: Amanda Towler
  - Co-PI: Devin Ellis
  - Researchers: Ruthanna Gordon, Mike Bunting, Brian Pierce, Michelle Morrison, Tess Wood, Kathleen Stewart, James Hull
  - Subawardees: Mirabolic, Inc.

Project Description

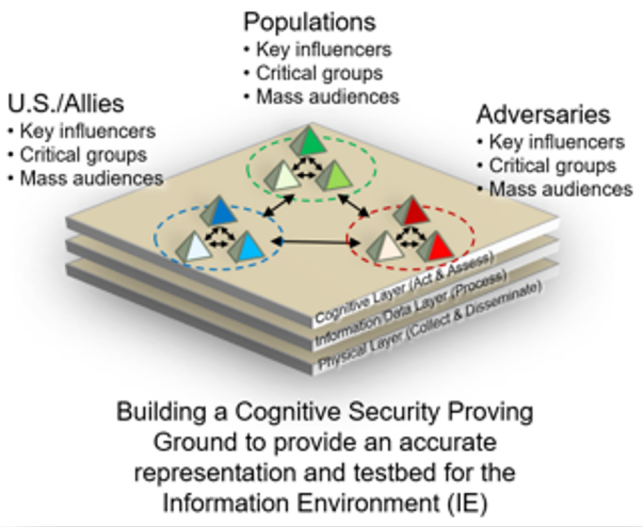
The INCAS Program will develop analyst-guided techniques and tools to detect and track geopolitical influence campaigns with quantified confidence. ARLIS will support the evaluation of performers, systems, tools, and models by leveraging our DoD- and IC-wide network of operators and our Cognitive Security Proving Ground (CSPG) suite of tools and methodologies.

Goal: *ARLIS will build a first-of-kind evaluation methodology and framework to assess the effectiveness of new and existing IO capabilities.*

Expected Impact: *If successful, our T&E environment will represent a revolutionary advance in the state of the art for evaluating IO tools and analytics.*

Success measures: *Does our hybrid approach to dataset generation facilitate more granular evaluation metrics? Does our simulation environment facilitate running parallel experiments and measuring reproducibility?*

INCAS T&E Overview



Building a Cognitive Security Proving Ground to provide an accurate representation and testbed for the Information Environment (IE)

- Hybrid approach based on Cognitive Security Proving Ground (CSGP)
- Combine historical data with synthetic data to meet ML-scale requirements
- Build simulation environment to both generate datasets and evaluate performer systems

Project is just starting, we are engaged with DARPA team and TA4 (program infrastructure and data team) to prepare for program kick off in August 2021

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Phase 1 Evaluation Scenarios	M1, M12	On sched
Phase 1 Annotated Datasets	M1, M10	On sched
v1 Simulation Environment + Participants	M6	On sched
Operational Stakeholders Group	M3	On sched
SME Group	M3	On sched

- **Big Wins (so far)**: Coordination with TA4 team
- **Transition goals/obstacles**: N/A
- **New ideas and whitepapers**: N/A
- **Sponsor relationship, new/additional sponsors**: N/A

Thank you!

Amanda Towler

atowler@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Applied AI, Automation, and Augmentation

AAA Mission Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

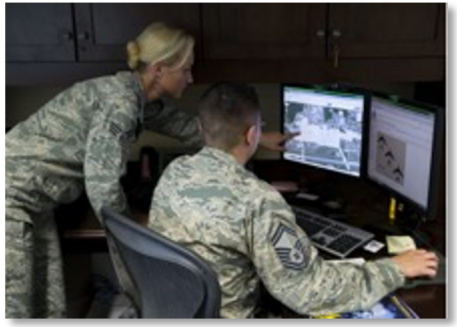
Artificial Intelligence, Automation, and Augmentation (AAA) Program

Craig Lawrence

clawren4@umd.edu

Mission Area Objectives: Operationalizing Artificial Intelligence, Autonomy, and Augmentation (AAA)

- Mission- and human-centered analysis and evaluation
  - Operational test, evaluation, verification, and validation (TEVV) with direct user engagement and mission data
  - Workflow analysis and mission modeling
- Systems engineering
  - System architecture and integration support
  - Integrated system TEVV
  - Security: certify robustness through adversarial methods and red teaming
- Research and development
  - Advancing TEVV for AI and autonomy – e.g., formal methods, simulation-based verification
  - Human-machine teaming
  - Prototype and demonstrate next generation cognitive augmentation – e.g., blended reality displays



Current Portfolio (1 of 3)

- DARPA/MTO Autonomy Application and Engineering Exploratorium (A2E2)
  - Software Defined Hardware (SDH)
  - Hierarchical Identify Verify Exploit (HIVE)
- OUSD(I&S) Artificial Intelligence, Automation, and Augmentation Program
  - AAA Testbed
  - HCI Lab
- OUSD(I&S) Algorithmic Warfare Core Function Team
  - Project Maven – Captured Enemy Materials Line of Effort
  - Project Maven – Information Environment Line of Effort
- ODNI Augmenting Intelligence with Machines (AIM)
  - AI Engineering Initiative
  - Partnership with CMU/SEI

Current Portfolio (2 of 3)

- DARPA/ACO - Adaptive warfighting architectures
  - System engineering effort looking at decision making architectures for classified application
- Army Research Lab (ARL) – AI and Autonomy for Multi-Agent Systems (ArtIAMAS)
  - Campus-led cooperative agreement with ARL – UMCP and UMBC
  - Advances dual-use solutions that address the Army's evolving needs for enabling AI and autonomy in complex environments
  - ARLIS is the lead on two projects, supporting two others
- INSURE Consortium Projects
  - NSA Human Machine Ecosystem Laboratory (HMEL) – Texas A&M University
  - SAF/CDM Expanding Applications for AAA – Texas A&M University
  - R&E/HBCU Office Cyber assessment of AI/ML tools – Howard and Morgan State
  - R&E/HBCU Office AI/ML Systems Engineering Workbench – Morgan State and Howard
  - R&E/HBCU Office ML Experimentation - UDC

Current Portfolio (3 of 3)

- OSD/Strategic Capabilities Office (SCO) Studies
  - Logistics and sustainment
  - Leadership decision-making modeling
- AFRL/RI – Fight Tonight
  - Shape requirements for Command and Control Vanguard Program
- NGA Anticipatory Ground-Level Imagery Analytics
  - Run through UMD CATT Laboratory

Artificial Intelligence, Automation, and Augmentation (AAA) Program

- **Task Order Sponsor:** OUSD(I&S)
- **Program Manager/Client:** Amanda McGlone
- **Period of Performance:** 22 May 2020 – 30 November 2021
  - No-cost extension through 28 February 2022 requested
- **TRL of the work:** 2 → 6
- **Total Budget:** $1.6M
- **Expenditures to date:** $422K (through March)

Team Members

- PI: Craig Lawrence
  - Testbed lead – Jana Schwartz
  - HCI Lab lead – Susan Campbell
- ARLIS Team Members:
  - Breanna Carter
  - Melissa Carraway (starting 10 May)
  - Victoria Chang
  - Valerie Karuzis
  - Susannah Paletz
  - Joshua Poore
  - Kelsey Rassmann (CS RA)
  - Samantha Tang (CS undergrad)

Project Description

- **Task 1 – Prototype AAA Testbed**
  - Develop methodologies and best practices for operational and system level testing of AAA technologies
  - Identify use case(s) and prototype “testbed”
  - Experiment with prototype testbed to refine methodologies
  - Hold workshops to help identify best of breed methodologies
- **Task 2 – Human Computer Interaction Lab**
  - Build out physical lab in ARLIS SCIF for the study of human computer interaction
  - ARLIS focus: Intel analysts using applications on desktop computers, Human-machine teaming, AR/VR

Operational Impact

"For example, if U.S. Special Operations Command uses a deep learning algorithm to translate documents from a raid on a terrorist compound and finds time-sensitive information, how do you measure **operational impact**?

Determining impact isn't just about statistical analysis on the level of precision-recall, but the impact compared to a human being's ability and the efficiency created for the operator." (Flournoy 2020)

Michele Flournoy, Avril Haines, Gabrielle Chefitz, *Building Trust Through Testing*, WestExec Advisors Report, 2020.

Challenge 1: Use Mission-Centered Metrics

Today AI TEVV is focused on model-level testing

- Produces a ROC curve of false positives vs true positives
- Great for comparing performance between algorithms, against a single dataset (aka mission)
- Doesn't tell us about performance across the mission space

Instead, the data should demonstrate the performance of the AI across the span of mission parameters

- Gold test set: validates training data
- Robust test set: relevant data *not* trained on
- Key cases: edges, corners, critical, or known-hard conditions

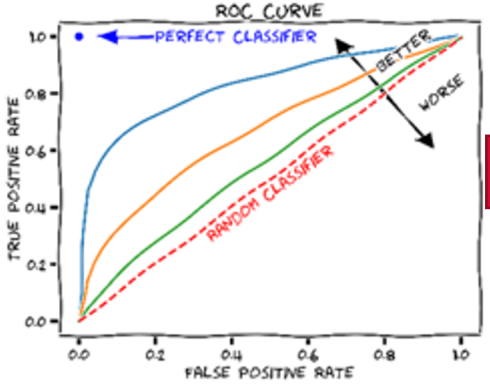
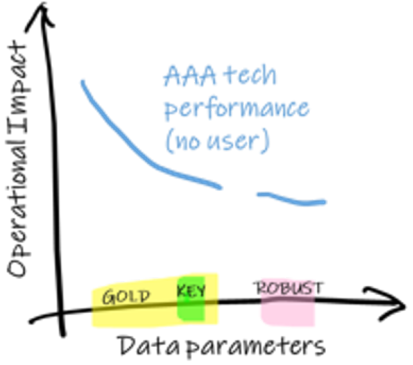


Figure from https://en.wikipedia.org/wiki/Receiver_operating_characteristic#/media/File:Roc-draft-xkcd-style.svg

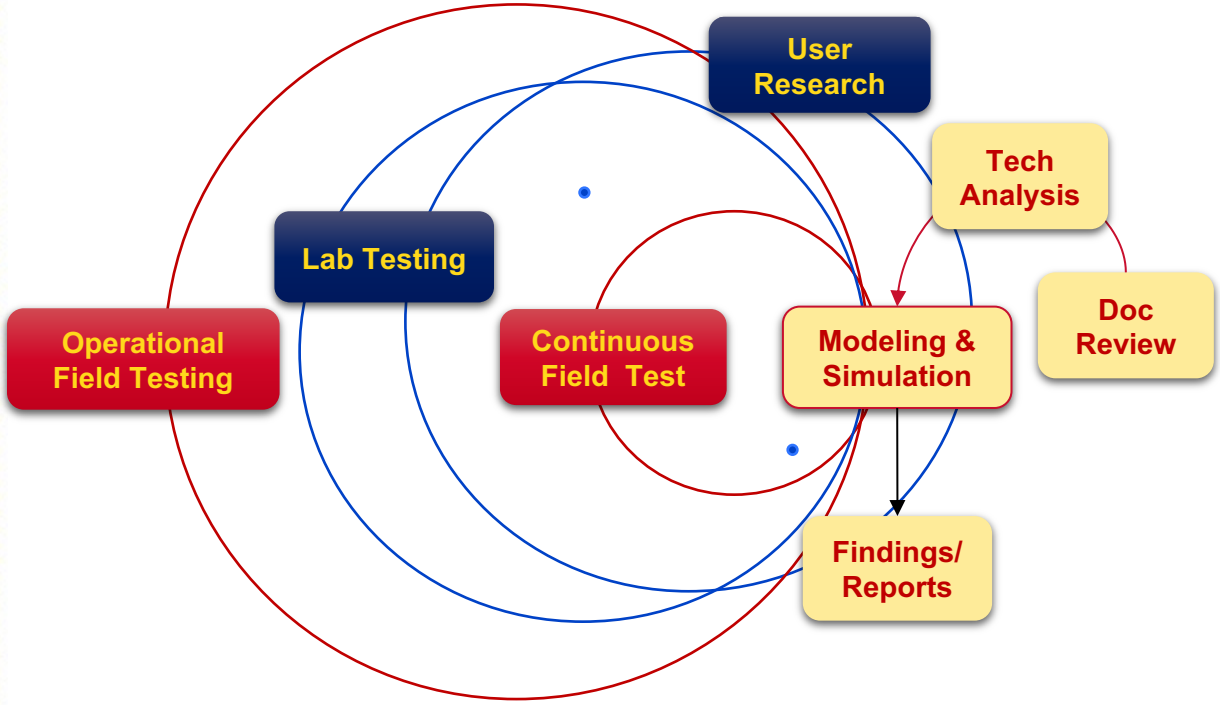


Challenge 2: Apply the best suite of methods to evaluate against those metrics

	Operational test in the field	Operational continuous use capture	Lab experiment with users	Lab experiment with proxy	Online experiment with proxy	Simulation
Mission realism	*****	*****	***	***	*	***
User realism	*****	*****	****	***	*	*
Data quality	****	***	*****	*****	*	**
Sample size	*	****	**	***	****	*****

"If I can test only one condition in the field, what should it be?"

Systematic, Spiraled, User-Centered TEVV



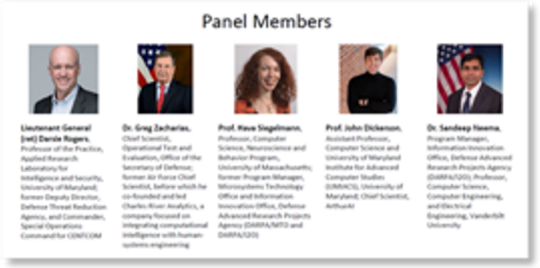
- Apportions test activities to suitable sites, based on fidelity, user-access, and risk
- Leverages multi-site/cohort testing to continually refine testing priorities at each sites
- Creates opportunities for both event-driven (e.g., visits, exercises) and continuous data collection

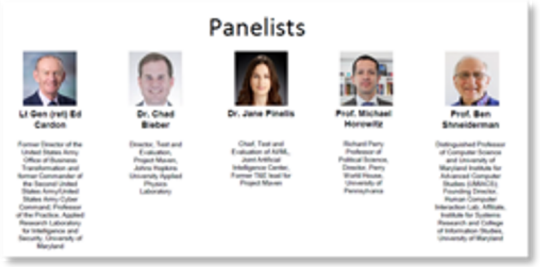
Use Cases / Stakeholders

- JAIC – Project Gargoyle
  - Base protection – near ground level video data
  - POC: Lt Col Brian Woolley
- NGA-R
  - Volunteered Geographic Information (VGI) fused with AI for increased trust
  - Immersive World (headset-based Virtual Reality data visualization)
  - POC: Joeanna Arthur
  - VGI use case will also be used on NGA-R GeoCog program
- USASOC - Information Warfare Center
  - Social media, …
  - POC: CPT Lindsay Gabow
- JSOC - Next Generation PED Lab
  - Classified application
  - POC: Lt Col Mike Blue

Workshop: "Should You Rely On That AI?"

- Virtual workshop held 28 January 2021
  - Over 170 participants!
  - Slides and videos posted: https://www.arlis.umd.edu/wksp202101-rely-on-ai
- Session 1: Role of simulation, test, training, qualifications, assurance cases in operational testing
- Session 2: Moving to a full-lifetime testing approach
- Session 3: A new look at policy, standards, and metrics specification
- Next Steps
  - Generate a workshop report





Task 1 Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Conduct literature review and document best of breed	3Q CY20	Green
Identify mission partner and analyst workflow	4Q CY20	Green
Stand up prototype testbed	1Q CY21	Yellow
Perform experiments in prototype testbed	2-3Q CY21	Yellow
Conduct workshops	1Q CY21, 3Q CY21	Green

Project Risk Assessment

- COVID-19 has shifted compressed schedule and shifted to the right
- We have spent lightly in anticipation of ramping up in FY21, and recommend a NCE

HCI Lab

- Given: Advanced research project building AI-based capability for analysis
- Goal: Understand how well human analysts can use that capability
  - Does it work for an individual? Does it work for collaboration?
- Generate metrics and assess performance and other key indicators
  - Cognitive load, attention to specific elements, satisfaction with the tool

HCI Lab Updates

- Planning now for multiple HCI labs
  - High side – RPB1, room 1218
  - Low side – Patapsco
  - (optional) “Travel” kit
- Eliciting constraints from ARLIS IT and Security to inform initial design for iteration
  - Main concerns are around video/audio recording
  - May require coordination with OUSD(I&S) before purchasing equipment
- Gathering sample requirements from existing AAA use cases to verify that plans meet existing requirements
  - Focus now is on VGI use case
- Planning to schedule workshop following UMD HCIL annual symposium (late May 2021)

Task 2 Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Detailed cost proposal for hardware and space	2Q CY21	Green
Technical report documenting initial capabilities	3Q CY21	Green
Workshop on HCI	2Q CY21	Green

Project Risk Assessment

- COVID-19 has shifted compressed schedule and shifted to the right
- We have spent lightly in anticipation of ramping up in FY21, and recommend a NCE

Schedule

			JFM	AMJ	JAS	OND	JFM
Task (lead researcher)	CY20 Q3	CY20 Q4	CY21 Q1	CY21 Q2	CY21 Q3	CY21 Q4	CY22 Q1
AAA T&E bootstrapping ;)							
HCIL development (Susan)							
JAIC Gargoyle (Josh)							
BIG INTERNAL DESIGN REVIEW							
NGA VGI (Polly + Breana)							
NGA Immersive World (? + Victoria)							
HCIL experiment (any one use case)							
USASOC IWC (Jana + ?)							
JSOC JIB (Jana + ?)							
Maven							
Document awesome approach							
Workshops						?	

Thank you!

Craig Lawrence
clawren4@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

AI Engineering Initiative

Craig Lawrence

clawren4@umd.edu

AI Engineering Initiative

- Sponsor: ODNI, Sub-award to CMU/SEI
- Program Manager/Client: Tom Drayer (ODNI)
- Period of Performance: November 16, 2020 - August 31, 2022
- TRL of the work: N/A
- Total Budget (+ Expenditures to Date): $1M
  - Expenditures to date: $42K
- Team Members:
  - PI – Craig Lawrence
  - Josh Poore
  - Erin Fitzgerald
  - Others TBD – pending stud topic selection

Project Description

- **Goal:** Support ODNI in growing a *National AI Engineering Initiative* focused on maturing an AI Engineering framework and discipline
- Task 1 - Work with CMU/SEI in support of ODNI to define the AI Engineering Initiative
  - Development of multi-year AI Engineering R&D Roadmap
  - Help ODNI build an effective coalition
  - ODNI looking for a “pipeline of capabilities”
- Task 2 - Research & development to advance/mature AI Engineering discipline
- Task 3 - Host summer internship program
  - Grow the talent pipeline

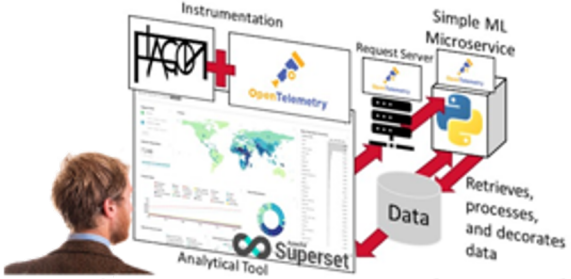
Growing the AI Engineering Initiative

- CMU/SEI has been working this since the fall
  - Defining the “Pillars of AI Engineering” strategy papers
  - Community building and engagement
    - Establish steering committee
    - Web presence (plus other social media, mailing lists
    - Engagement plan / value proposition for all constituencies
    - Prepare / execute “hard launch”
  - Workshops / training
- ARLIS is supporting as we ramp up this spring
  - ODNI - interested in leveraging the ARLIS INSURE consortium

Proposed Study Topics

Understanding AI Influence on User Tasking and User Trust through Software Instrumentation and System Telemetry

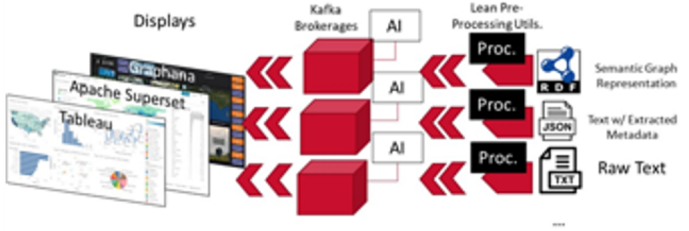
- **Background**: Subjective assessments of human-AI interactions abstract away influence of AI generated information within and across operational workflows
- **Objective**: In pilot testing, assess utility of software instrumentation and system telemetry in assessing the impact of AI on user tasking:
  - Prototype metrics of task efficiency using
  - Prototype methods for extracting traces of AI outputs embedded in user workflow (e.g., filter, query terms)
  - Prototype metrics for establishing the influence of AI information relative to other information in workflows
  - Cross-Validate metrics against established surveys (e.g., trust, SUS, etc.)



Comprehensive instrumentation and system telemetry tracks how and how much user relies on AI output

Exploring Reusable & Recombinant AI/ML via flexible data engineering pipelines and efficient Data Service architectures

- **Background**: The IC has significant investments in AI/ML and other analytical automation
  - Many of these capabilities are embedded in applications or stand-alone suites
  - Repurposing to serve different CONOPs or work efficiently with new data sources often requires significant level of effort

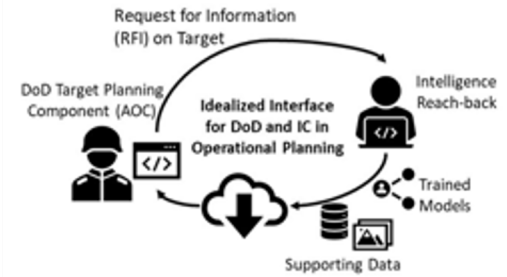


Flexible data engineering pipelines cultivate reusable utilities that reduce the obsolescence of existing AI

- **Objective**: Develop proof of concept experiments to demonstrate efficiency, scalability, and generalizability of reusable utilities for flexible data engineering pipelines in a domain-relevant use-case
  - Perform use-case driven experiments to serve existing AI/analytics new (or legacy) data
  - Perform TEVV to verify the reliability of repurposed AI
  - Propose, Recommend efficiency Metrics for TEVV
  - Recommend acquisition strategy, packaging for reuseable pre-processing, translation utilities

Ensuring Joint-Services Analytical Interoperability through Data Service and Knowledge Management

- **Background**: Interoperability in data and models is critical for leveraging AI effectively in Joint-Services Operations (JADO, MDO, JADC2)
  - Future intelligence products may rely on AI outputs, or may themselves be models
  - These products may themselves serve as inputs to operational workflows



AI Engineering needs to take into account technical interoperability between services to accelerate operations and replace manual workflows.

- **Objective**: Deliver recommendations for maintaining IC flexibility in meeting mission needs while retaining interoperability platform and system ops with DoD operations
  - Leverage points of access with DoD (Kessel Run (Enterprise AI portfolio, and PlatformOne)
  - Document core operating concepts for deploying and managing AI into applications and operations
  - Develop candidate joint-agency use-cases
  - Provide high level recommendations for maintaining IC<>DOD interoperability

IC Summer of Code

- **Background**: Modern application, service, and analytical development are inspired by open-source models development models
  - They encourage generalization, resource sharing, and hardening through co-development and community development
  - To spur essential AI Engineering infrastructure and rapidly build capabilities and process, adopt models like Google's Summer of Code
- **Objective**: Deliver recommendations on how to stage large, IC-wide initiatives to spur capability exposure and co-development. Including the necessary infrastructure and candidate use-cases to guide development at different levels of security
  - Leverage points of access with USG stakeholders in open-source development and infrastructure (NASA-JPL, and PlatformOne)
  - Develop example agency-specific use-cases that may be viable to spur development at different levels of security.
  - Document industry models (e.g., Google Summer of code) identifying necessary resources for staging such events
  - Identify mechanisms and program in the IC that would allow for staff/development engagement within the IC

RISC Internship Topics

- ODNI provided a long list of potential topics
  - Developed by MITRE
  - Opportunity to work with MITRE to obtain data and testbed

- ARLIS generated a list of five topics for consideration
  - Two based on MITRE-generated topics
  - Three based on study topics
  - ODNI prioritized the topics in this list

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Define and kick off studies	2Q21	On sched
Develop internship topics	1Q21	Delayed
Workshop	3Q21	On sched

Project Risk Assessment

- Staffing for studies
  - Mitigation: Exploring multiple options with teaming (including via INSURE Consortium)

Next Steps and Future Capabilities

- Continue to work with CMU/SEI on AI Engineering Initiative
  - Workshops, outreach, planning, ….
- Studies
  - Finalize scope of work for studies
  - Build teams and begin execution
- Internship
  - Refine ODNI-provided topics
  - Support internship execution

Thank you!

Craig Lawrence

clawren4@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Anticipatory Ground-Level Imagery Analytics (AGLIA)

Michael Pack
PackML@umd.edu

Rama Chellappa
chella@umd.edu

AGLIA

- **Sponsor:** NGA
- **Program Manager/Client:** Veda Bharath
- **Period of Performance:** 3 years (9/30/2019 – 9/29/2022)
- **Funding type:** R&D
- **Core Team Members:** Michael Pack, Rama Chellappa, Co-PI & Don Woodbury

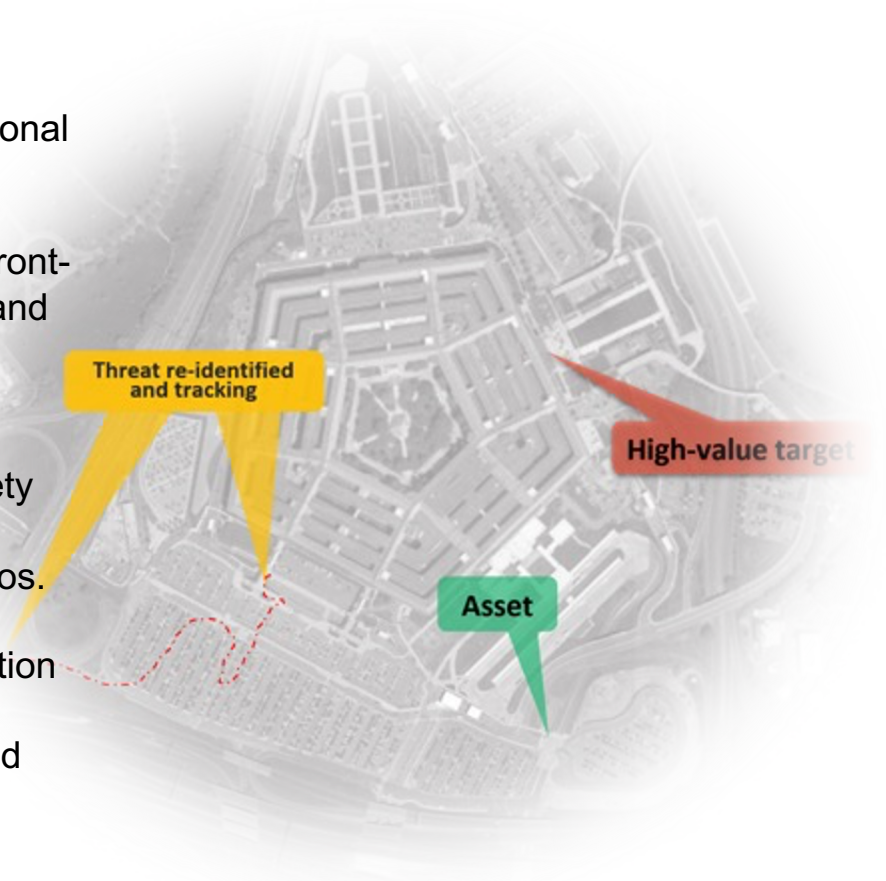
Project Description

1. Demonstrate capabilities to enhance situational awareness at high value facilities

2. Perform fundamental research to develop front-end visualizations and analytics for image and video processing.

3. Fuse existing multivariate real-time data streams from transportation and public safety assets with new and emerging datasets derived from static images and motion videos.

4. Process and analyze fused data for correlation and threat detection—including providing visualizations and dashboards to aid in rapid analysis of these threats and provide automated alerting.



AGLIA UI Prototyping

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

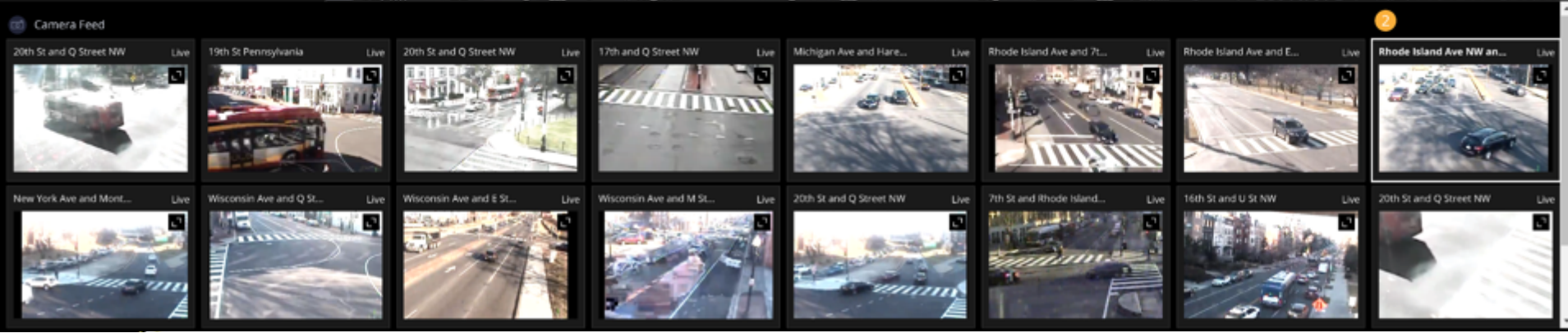
- [ ] Ambulance
- [ ] Bus
- [ ] Van

TYPE	ID	CAMERA LOCATION	LAST SEEN

No Vehicle Type Selected

Monitored Region

Camera Feed



AGLIA Project

Identified Vehicles

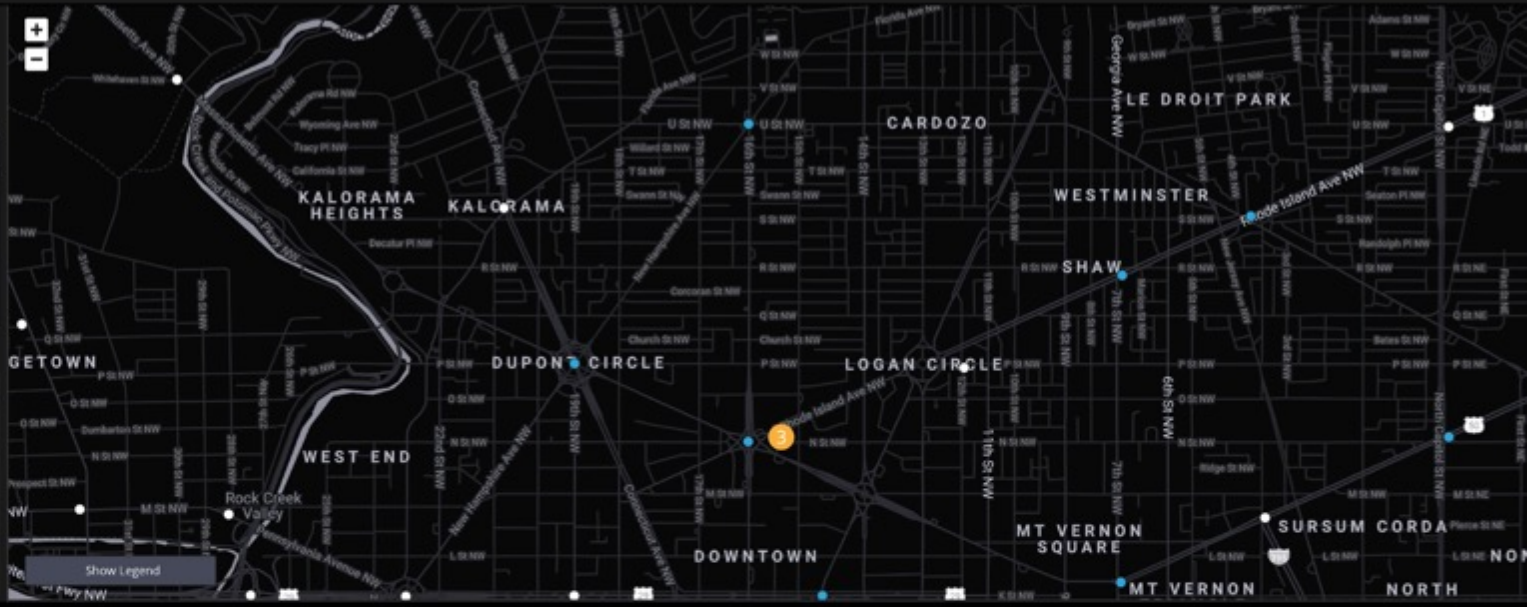
Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

12 vehicles IDed in 10m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B4	20th St and Q St. NW	24s ago
Bus	B3	19th St Pennsylvania	45s ago
Bus	B2	15th and K and Vermont	1m ago
Bus	B1	17th and Conn and K	1m ago
Bus	B9	Michigan Ave and Hare...	1m ago
Bus	B8	Rhode Island Ave and E...	3m ago
Bus	B7	Rhode Island Ave and E...	3m ago
Bus	B6	Georgia Ave and Irving St...	4m ago

Monitored Region



Camera Feed - Identified Buses

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

15 vehicles IDed in 14m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	27s ago
Bus	B4	20th St and Q St. NW	1m ago
Bus	B3	19th St Pennsylvania	1m ago
Bus	B2	15th and K and Vermont	2m ago
Bus	B1	17th and Conn and K	2m ago
Bus	B9	Michigan Ave and Hare...	4m ago
Bus	B8	Rhode Island Ave and E...	4m ago
Bus	B7	Rhode Island Ave and E...	5m ago

Monitored Region

1

Rhode Island Ave NW and 16th St NW — Live

2

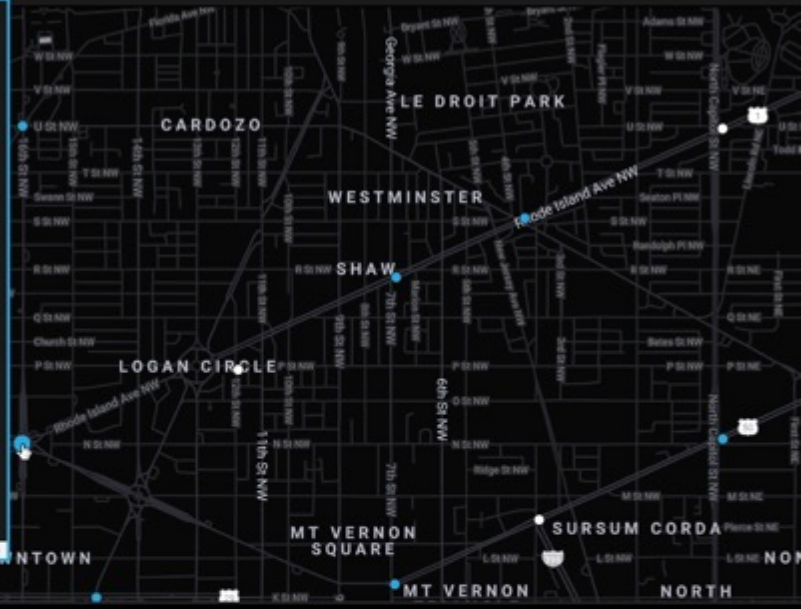
Number of Buses this Camera has IDed: 3 — More to the right...

B5 — 27s ago

00:00:02 — 2:56 PM 10/01/20

B6 — 6m ago

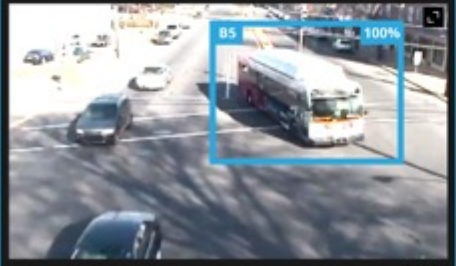
00:00:03 — 2:53 PM 10/01/20



Camera Feed - Identified Buses

4

Rhode Island Ave and 16th St NW — 27s ago

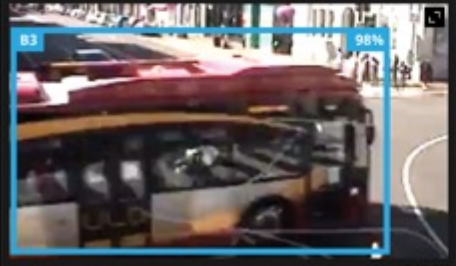


00:00:02 — 2:56 PM 10/01/20

20th St and Q Street NW — 1m ago

00:00:02 — 2:56 PM 10/01/20

19th St Pennsylvania — 1m ago



00:00:03 — 2:55 PM 10/01/20

15th and K and Vermont — 2m ago

00:00:04 — 2:55 PM 10/01/20

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

15 vehicles IDed in 14m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	27s ago
Bus	B4	20th St and Q St. NW	1m ago
Bus	B3	19th St Pennsylvania	1m ago
Bus	B2	15th and K and Vermont	2m ago
Bus	B1	17th and Conn and K	2m ago
Bus	B9	Michigan Ave and Hare...	4m ago
Bus	B8	Rhode Island Ave and E...	4m ago
Bus	B7	Rhode Island Ave and E...	5m ago

3

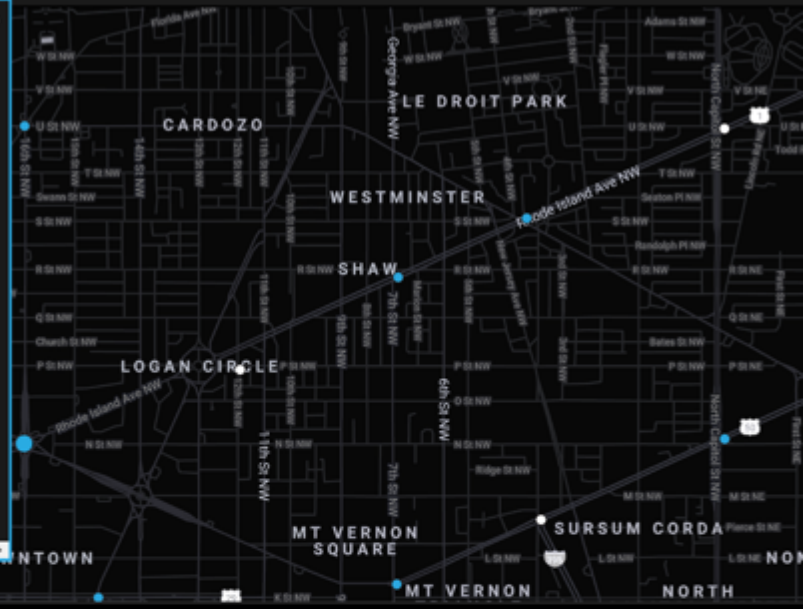
Monitored Region

Rhode Island Ave NW and 16th St NW Live

Number of Buses this Camera has IDed: 3 More to the right...

B5 27s ago B6 6m ago

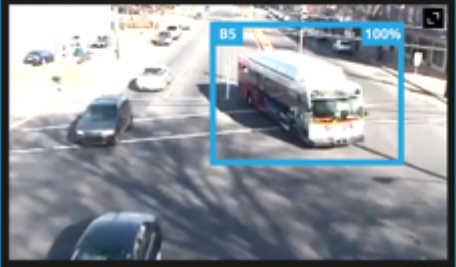
00:00:02 2:56 PM 10/01/20 00:00:03 2:53 PM 10/01/20



Camera Feed - Identified Buses

2

Rhode Island Ave and 16th St NW 27s ago

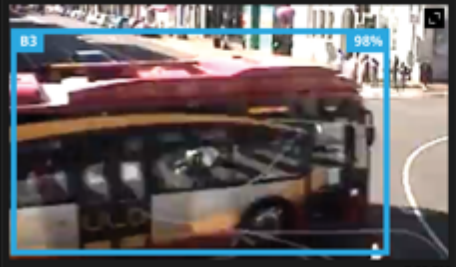


00:00:02 2:56 PM 10/01/20

20th St and Q Street NW 1m ago

00:00:02 2:56 PM 10/01/20

19th St Pennsylvania 1m ago



00:00:03 2:55 PM 10/01/20

15th and K and Vermont 2m ago

00:00:04 2:55 PM 10/01/20

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

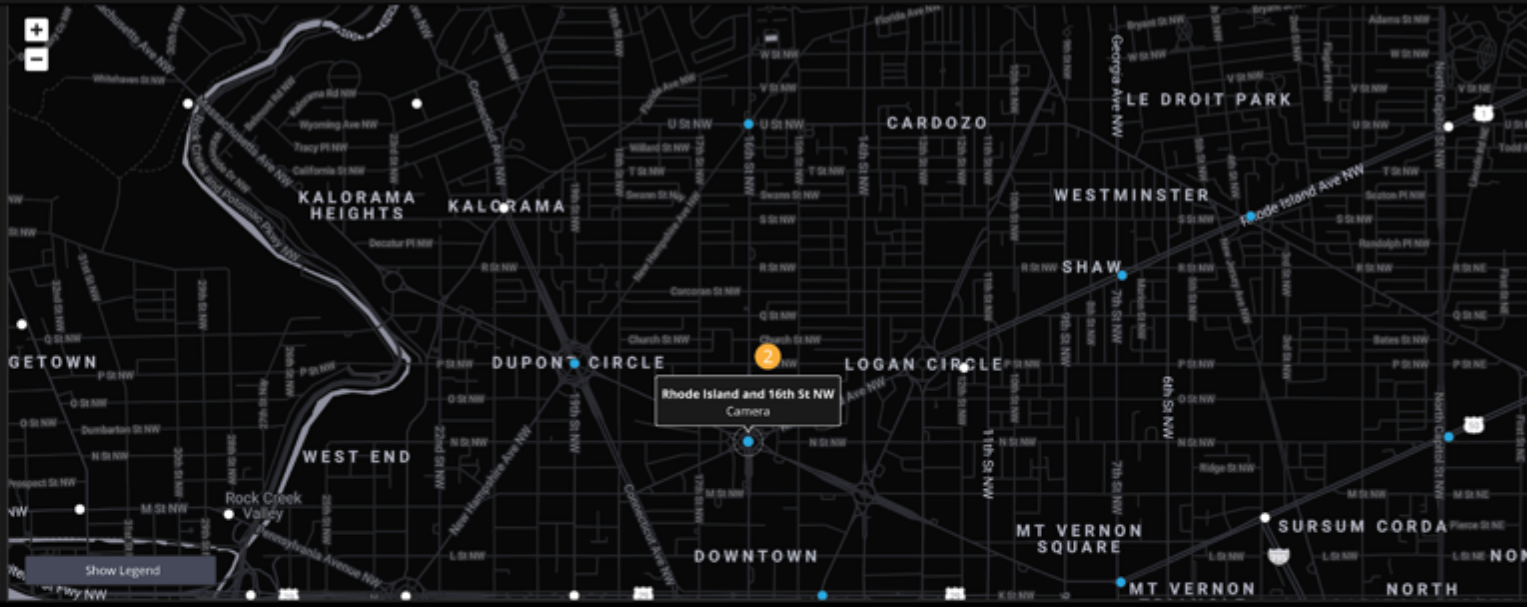
15 vehicles IDed in 14m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	27s ago
Bus	B4	20th St and Q St. NW	1m ago
Bus	B3	19th St Pennsylvania	1m ago
Bus	B2	15th and K and Vermont	2m ago
Bus	B1	17th and Conn and K	2m ago
Bus	B9	Michigan Ave and Hare...	4m ago
Bus	B8	Rhode Island Ave and E...	4m ago
Bus	B7	Rhode Island Ave and E...	5m ago

1

Click to start tracking this vehicle.

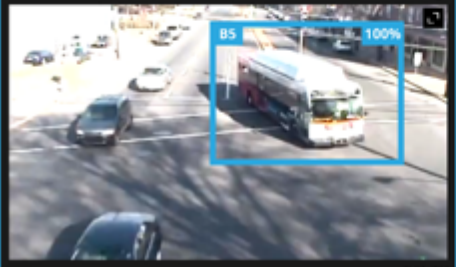
Monitored Region



Camera Feed - Identified Buses

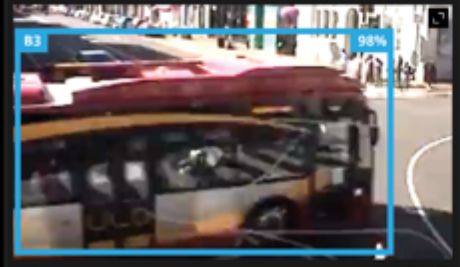
3

Rhode Island Ave and 16th St NW — 27s ago



20th St and Q Street NW — 1m ago

19th St Pennsylvania — 1m ago



15th and K and Vermont — 2m ago

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

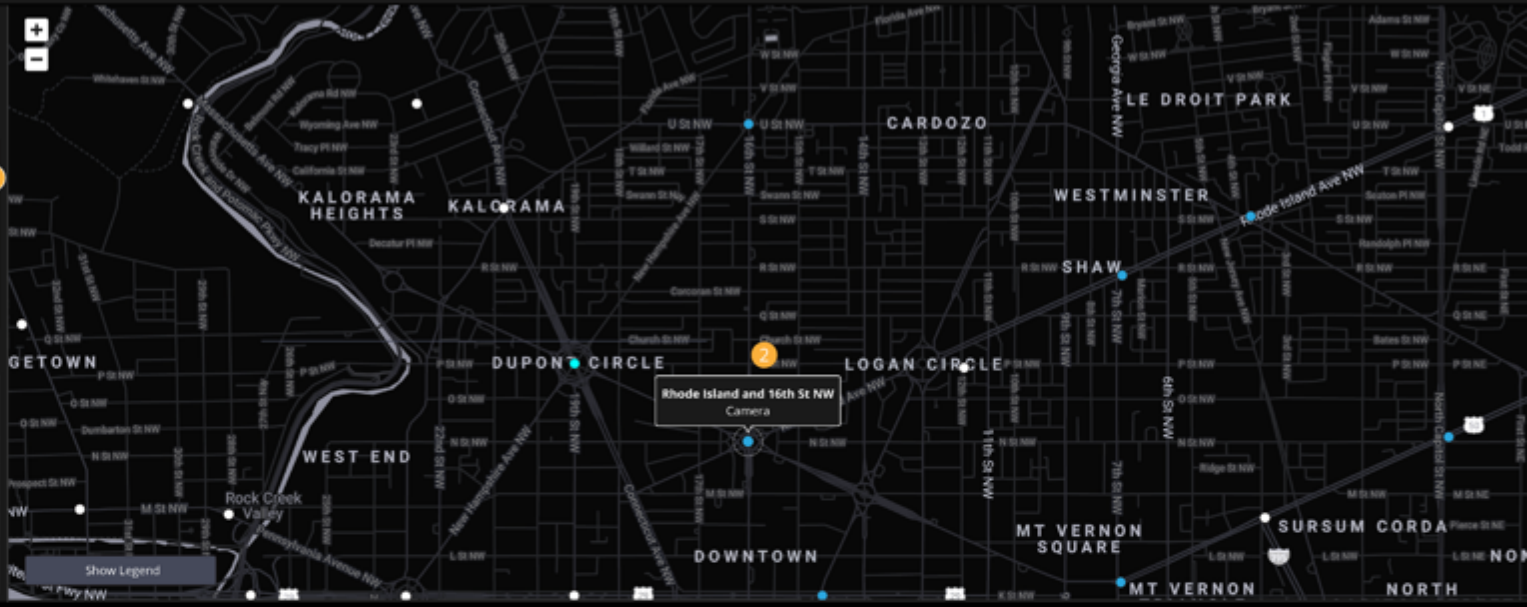
☐ Ambulance ☑ Bus ☐ Van

15 vehicles IDed in 14m

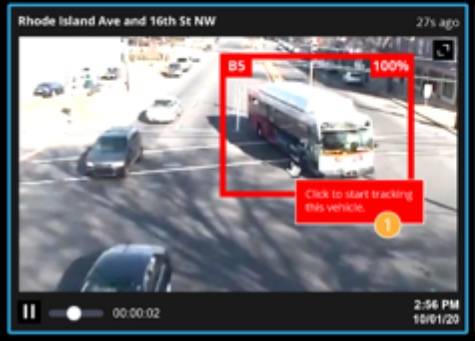
TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	27s ago
Bus	B4	20th St and Q St. NW	1m ago
Bus	B3	19th St Pennsylvania	1m ago
Bus	B2	15th and K and Vermont	2m ago
Bus	B1	17th and Conn and K	2m ago
Bus	B9	Michigan Ave and Hare...	4m ago
Bus	B8	Rhode Island Ave and E...	4m ago
Bus	B7	Rhode Island Ave and E...	5m ago

3

Monitored Region



Camera Feed - Identified Buses



AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

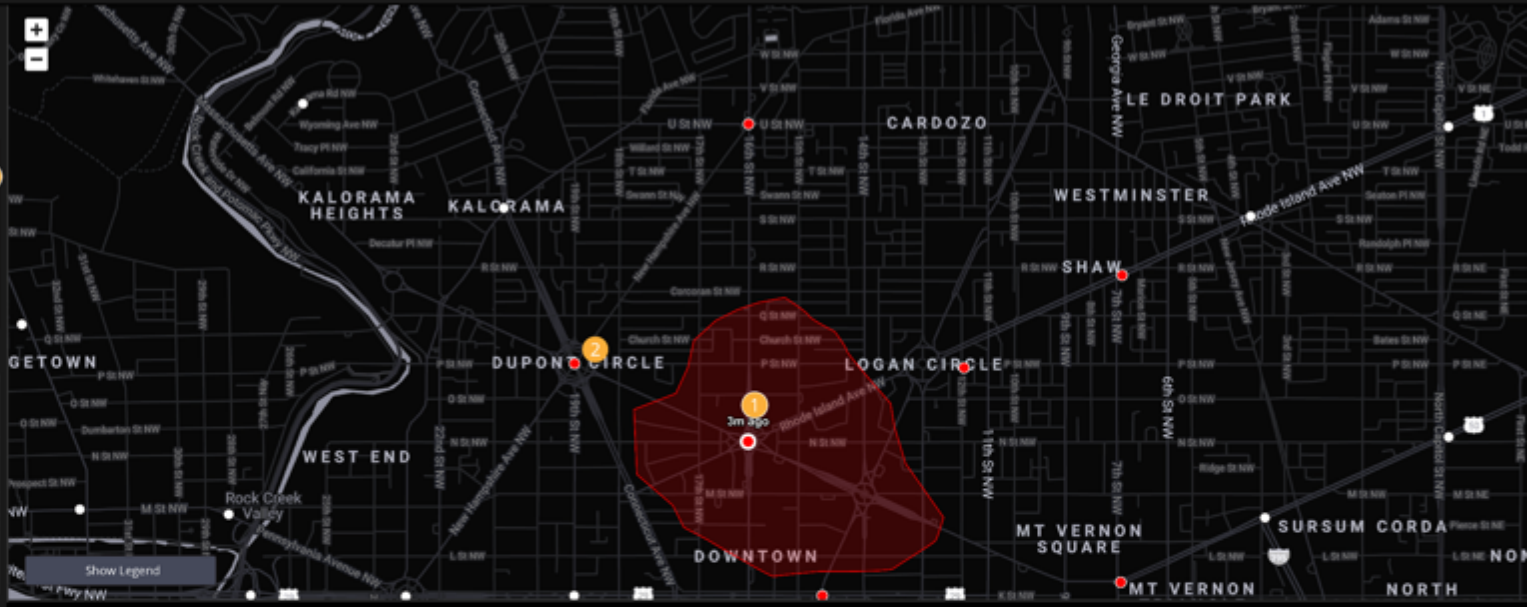
☐ Ambulance ☑ Bus ☐ Van

18 vehicles IDed in 17m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	3m ago
Bus	B4	20th St and Q St. NW	4m ago
Bus	B3	19th St Pennsylvania	5m ago
Bus	B2	15th and K and Vermont	5m ago
Bus	B1	17th and Conn and K	7m ago
Bus	B9	Michigan Ave and Hare...	9m ago
Bus	B8	Rhode Island Ave and E...	10m ago
Bus	B7	Rhode Island Ave and E...	12m ago

3

Monitored Region



1 2

Tracked Vehicle 4

Open Camera Tree

Bus - B5 Stop Tracking

Direction: **East** ID Score: **100%**

Speed: **35 mph** Tracking Score: -

List of Cameras Passed 5

Camera	Time Since Passed
Rhode Island Ave and 16 St NW	3 min

Most Recent Camera 6

Rhode Island Ave and 16th St NW — 3m ago

Predicted Cameras 7

16th St and U St NW — Live

Rhode Island Ave and E... — Live

Georgia Ave and Irving St... — Live

16th St and U St NW — Live

Georgia Ave and Irving St... — Live

Georgia Ave and Irving St... — Live

Rhode Island Ave and E... — Live

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

18 vehicles IDed in 17m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	3m ago
Bus	B4	20th St and Q St. NW	4m ago
Bus	B3	19th St Pennsylvania	5m ago
Bus	B2	15th and K and Vermont	5m ago
Bus	B1	17th and Conn and K	7m ago
Bus	B9	Michigan Ave and Hare...	9m ago
Bus	B8	Rhode Island Ave and E...	10m ago
Bus	B7	Rhode Island Ave and E...	12m ago

Monitored Region

Tracked Vehicle

Open Camera Tree

Bus - B5 — Stop Tracking

Direction: **East** ID Score: **100%**

Speed: **35 mph** Tracking Score: -

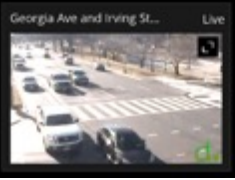
List of Cameras Passed

Camera	Time Since Passed
Rhode Island Ave and 16 St NW	**3 min**

Most Recent Camera

Rhode Island Ave and 16th St NW — 3m ago

Predicted Cameras



AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

19 vehicles IDed in 21m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and 1...	7m ago
Bus	B4	20th St and Q St. NW	8m ago
Bus	B3	19th St Pennsylvania	9m ago
Bus	B2	15th and K and Vermont	9m ago
Bus	B1	17th and Conn and K	11m ago
Bus	B9	Michigan Ave and Hare...	13m ago
Bus	B8	Rhode Island Ave and E...	14m ago
Bus	B7	Rhode Island Ave and E...	16m ago

Monitored Region

Tracked Vehicle

Open Camera Tree

Bus - A — Stop Tracking

Direction: NE — ID Score: 100%

Speed: 35 mph — Tracking Score: -

List of Cameras Passed

Camera	Time Since Passed
Rhode Island Ave and 16 St NW	7m ago

Most Recent Camera

Rhode Island Ave and 16th St NW — 7m ago

Predicted Cameras

16th St and U St NW — Live

Rhode Island Ave and E... — Live

Georgia Ave and Irving St... — Live

16th St and U St NW — Live

Georgia Ave and Irving St... — Live

Georgia Ave and Irving St... — Live

AGLIA Project

Identified Vehicles

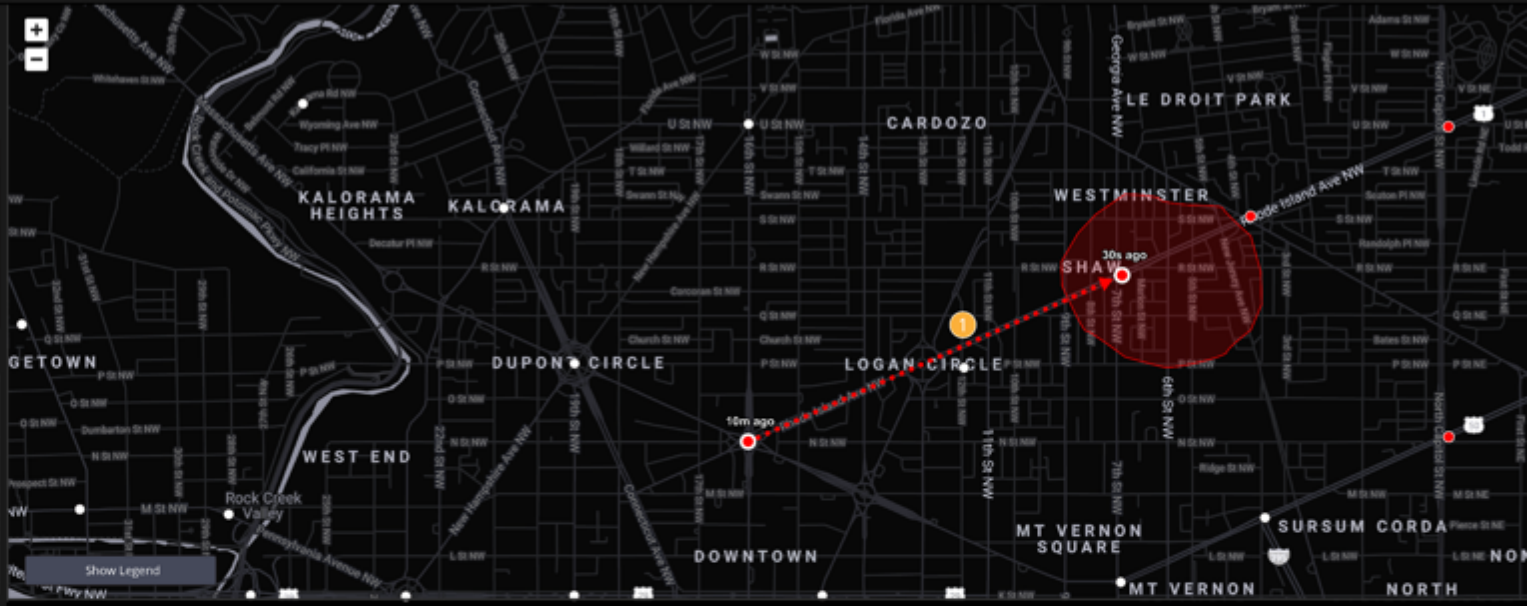
Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

20 vehicles IDed in 24m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	Rhode Island Ave and F...	30s ago
Bus	B6	16th St and U St NW	1m ago
Bus	B4	20th St and Q St. NW	5m ago
Bus	B11	19th St Pennsylvania	6m ago
Bus	B2	15th and K and Vermont	7m ago
Bus	B1	17th and Conn and K	7m ago
Bus	B9	Michigan Ave and Hare...	8m ago
Bus	B8	Rhode Island Ave and E...	8m ago

Monitored Region



Tracked Vehicle

Open Camera Tree

Bus - B5 — Stop Tracking

Direction: **NE** ID Score: **100%**

Speed: **35 mph** Tracking Score: **98%**

List of Cameras Passed

Camera	Time Since Passed
Rhode Island Ave and Florida Ave	30s ago
Rhode Island Ave and 16 St NW	10m ago

Last Camera Passed

Rhode Island Ave and 1... 10m ago

Most Recent Camera

Rhode Island Ave and Florida Ave 30s ago

Predicted Cameras

16th St and U St NW Live

Rhode Island Ave and E... Live

Georgia Ave and Irving St... Live

AGLIA Project

Identified Vehicles

Identify the following vehicles when they pass a camera:

☐ Ambulance ☑ Bus ☐ Van

20 vehicles IDed in 25m

TYPE	ID	CAMERA LOCATION	LAST SEEN
Bus	B5	N. Cap and NY	1m ago
Bus	B6	16th St and U St NW	1m ago
Bus	B4	20th St and Q St. NW	5m ago
Bus	B11	19th St Pennsylvania	6m ago
Bus	B2	15th and K and Vermont	7m ago
Bus	B1	17th and Conn and K	7m ago
Bus	B9	Rhode Island Ave and F...	8m ago
Bus	B8	Rhode Island Ave and E...	8m ago

Monitored Region

Tracked Vehicle

Open Camera Tree

Bus - B5 — Stop Tracking

Direction: S — ID Score: 100%

Speed: 35 mph — Tracking Score: 98%

List of Cameras Passed

1

Camera	Time Since Passed
N. Cap and NY	1m ago
Rhode Island Ave and Florida Ave	5m ago
Rhode Island Ave and 16 St NW	17m ago

Last 2 Cameras Passed

2

Rhode Island Ave and 1... 17m ago

00:00:02 2:53 PM 10/01/20

Rhode Island Ave and F... 5m ago

00:00:02 3:03 PM 10/01/20

Most Recent Camera

N. Cap and NY 1m ago

00:00:02 3:08 PM 10/01/20

Predicted Cameras

16th St and U St NW Live

Rhode Island Ave and E... Live

Georgia Ave and Irving St... Live

AGLIA Project

Tracked Vehicle 1

Bus - B5 — Stop Tracking

Direction: East — ID Score: 100%

Speed: 35 mph — Tracking Score: -

List of Cameras Passed 2

Camera	Time Since Passed
N. Cap and NY	00:01:23

List of Predicted Cameras 3

Camera	Should Pass In...
New Hampshire Ave @ 20th St	00:03:24
New Hampshire Ave @ 2nd St N...	00:11:53
22nd St NW @ N St NW	00:09:24
20th St NW @ N St NW	00:15:08
Connecticut Ave NW @ Rhode Islan...	00:01:04
20th St NW @ N St NW	00:13:37
Connecticut Ave NW @ K ST	00:15:46
16th St and Scott Cir NW	00:12:32
Massachusetts Ave	00:05:48
16th St and Scott Cir NW	00:08:21
New Hampshire Ave	00:01:15
New Hampshire Ave	00:18:37
Q St NW @ 17th St	00:15:19
18th St NW @ R St NW	00:19:26

Monitored Region 4

Management View

Camera Tree

Most Recent Camera 5

Bus - B5

N. Cap and NY — 00:01:23 ago

00:00:03 — 1:45 PM 10/01/20

00:03:24 — 0.5 miles

00:01:04 — 0.1 miles

00:05:48 — 1.4 miles

00:01:15 — 0.3 miles

6

7

00:11:53 — 0.8 miles

00:09:24 — 1.2 miles

00:15:08 — 0.5 miles

00:13:37 — 0.9 miles

00:15:46 — 1.6 miles

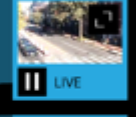
00:12:32 — 0.7 miles

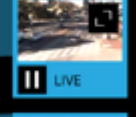
00:08:21 — 0.5 miles

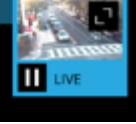
00:18:37 — 1.3 miles

00:15:19 — 1.2 miles

00:19:26 — 1.6 miles







AGLIA Project

Tracked Vehicle

Bus - B5 Stop Tracking

Direction: East ID Score: 100%

Speed: 35 mph Tracking Score: -

List of Cameras Passed

Camera	Time Since Passed
N. Cap and NY	00:02:38

List of Predicted Cameras

Cameras	Should Pass In...
New Hampshire Ave @ 20th St	00:03:13
New Hampshire Ave @ 2nd St N...	00:09:41
22nd St NW @ N St NW	00:07:44
20th St NW @ N St NW	00:13:38
Connecticut Ave NW @ Rhode Islan...	00:00:00
20th St NW @ N St NW	00:13:37
Connecticut Ave NW @ K ST	00:15:46
16th St and Scott Cir NW	00:12:32
Massachusetts Ave	00:04:54
16th St and Scott Cir NW	00:08:21
New Hampshire Ave	00:00:22
New Hampshire Ave	00:18:37
Q St NW @ 17th St	00:15:19
18th St NW @ R St NW	00:19:26

Monitored Region

Management View

Camera Tree

Most Recent Camera

Bus - B5

N. Cap and NY 00:02:38 ago

00:00:03 1:45 PM 10/01/20

00:03:13
0.5 miles

00:00:00
0.1 miles

00:04:54
1.4 miles

00:00:22
0.3 miles

00:09:41
0.8 miles

00:07:44
1.2 miles

00:13:38
0.5 miles

00:13:37
0.9 miles

00:15:46
1.6 miles

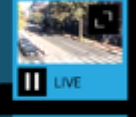
00:12:32
0.7 miles

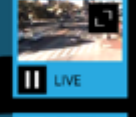
00:08:21
0.5 miles

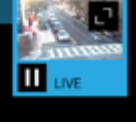
00:18:37
1.3 miles

00:15:19
1.2 miles

00:19:22
1.6 miles







AGLIA Project

Tracked Vehicle

Bus - B5 Stop Tracking

Direction: East ID Score: 100%

Speed: 35 mph Tracking Score: -

List of Cameras Passed

Camera	Time Since Passed
N. Cap and NY	00:02:48

List of Predicted Cameras

Cameras	Should Pass In...
New Hampshire Ave @ 20th St	00:03:13
New Hampshire Ave @ 2nd St N...	00:09:31
22nd St NW @ N St NW	00:07:34
20th St NW @ N St NW	00:13:28
Massachusetts Ave	00:04:54
16th St and Scott Cir NW	00:08:11
New Hampshire Ave	00:00:12
New Hampshire Ave	00:18:27
Q St NW @ 17th St	00:15:09
18th St NW @ R St NW	00:19:16

Monitored Region

Management View

Camera Tree

Most Recent Camera

Bus - B5

N. Cap and NY 00:02:48 ago

00:00:03 1:45 PM 10/01/20

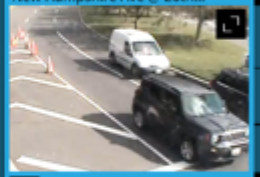
00:03:13
0.5 miles

00:04:54
1.4 miles

00:00:12
0.3 miles

1

New Hampshire Ave @ 20th...



LIVE 70%

Massachusetts Ave

LIVE 15%

New Hampsire Ave

LIVE 5%

2

00:09:31
0.8 miles

00:07:34
1.2 miles

00:13:28
0.5 miles

00:08:11
0.5 miles

00:18:27
1.3 miles

00:15:09
1.2 miles

00:19:12
1.6 miles


LIVE


LIVE


LIVE


LIVE


LIVE


LIVE


LIVE

AGLIA Project

Tracked Vehicle

Bus - B5 Stop Tracking

Direction: East ID Score: 100%

Speed: 35 mph Tracking Score: -

List of Cameras Passed

Camera	Time Since Passed
N. Cap and NY	00:06:01

List of Predicted Cameras

Cameras	Should Pass In...
New Hampshire Ave @ 20th St	00:00:12
New Hampshire Ave @ 2nd St N...	00:08:29
22nd St NW @ N St NW	00:06:00
20th St NW @ N St NW	00:11:44
Massachusetts Ave	00:01:13
16th St and Scott Cir NW	00:04:57

Monitored Region

Management View

Camera Tree

Most Recent Camera

Bus - B5

N. Cap and NY 00:06:01 ago

00:00:03 1:45 PM 10/01/20

00:00:12
0.5 miles

New Hampshire Ave @ 20th...

LIVE 80%

00:08:29
0.8 miles

LIVE

00:06:00
1.2 miles

LIVE

00:11:44
0.5 miles

LIVE

00:01:13
1.4 miles

Massachusetts Ave

LIVE 20%

00:04:57
0.5 miles

LIVE

AGLIA Project

Tracked Vehicle

Bus - B5 Stop Tracking

Direction: East ID Score: 100%

Speed: 35 mph Tracking Score: -

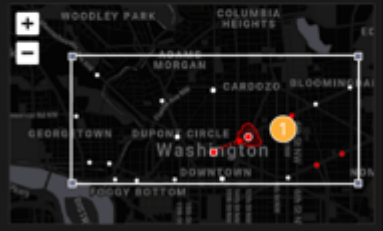
List of Cameras Passed

Camera	Time Since Passed
N. Cap and NY	00:06:04

List of Predicted Cameras

Cameras	Should Pass In...
New Hampshire Ave @ 20th St	00:00:09
New Hampshire Ave @ 2nd St N...	00:08:32
22nd St NW @ N St NW	00:06:03
20th St NW @ N St NW	00:11:47
Massachusetts Ave	00:01:16
16th St and Scott Cir NW	00:05:00

Monitored Region



Management View

Camera Tree

Most Recent Camera

Bus - B5

N. Cap and NY 00:06:04 ago

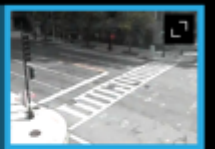
00:00:03 1:45 PM 10/01/20

00:00:09
0.5 miles

New Hampshire Ave @ 20th...

LIVE 80%

00:08:32
0.8 miles



LIVE

00:06:03
1.2 miles

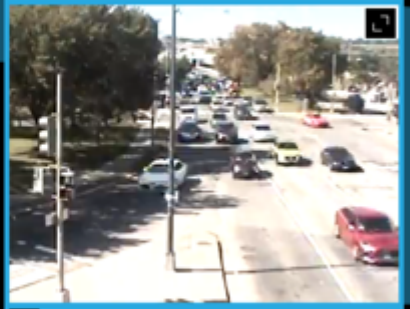
LIVE

00:11:47
0.5 miles

LIVE

00:01:16
1.4 miles

Massachusetts Ave



LIVE 20%

00:05:00
0.5 miles

LIVE

AGLIA Project

Tracked Vehicle

Bus - B5 Stop Tracking

Direction: South East ID Score: 100%

Speed: 35 mph Tracking Score: 95% 4

List of Cameras Passed

Camera	Time Since Passed
N. Cap and NY 1	00:06:02
New Hampshire Ave @ 20th St	00:00:1

List of Predicted Cameras

Cameras	Should Pass In...
Massachusetts Ave	00:08:19
New Hampshire Ave @ 2nd St N...	00:03:53
22nd St NW @ N St NW	00:09:24
Massachusetts Ave	00:05:50
16th St and Scott Cir NW	00:15:08
Massachusetts Ave	00:11:34
New Hampshire Ave @ 2nd St N...	00:13:37
22nd St NW @ N St NW	00:15:46

Monitored Region

Management View

Camera Tree

3

Cameras Passed

Most Recent Camera

Bus - B5

New Hampshire Ave @ 20th... 00:00:01 ago

00:00:03 1:47 PM 10/01/20

2

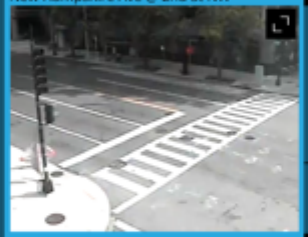
N. Cap and NY

00:08:19
0.8 miles

00:05:50
1.2 miles

00:11:34
0.5 miles

New Hampshire Ave @ 2nd St NW



LIVE 64%

22nd St NW @ N St NW

LIVE 24%

20th St NW @ N St NW

LIVE 12%

00:03:53
0.2 miles

00:09:24
0.6 miles

00:15:08
0.8 miles

00:13:37
0.9 miles

00:15:46
1.6 miles

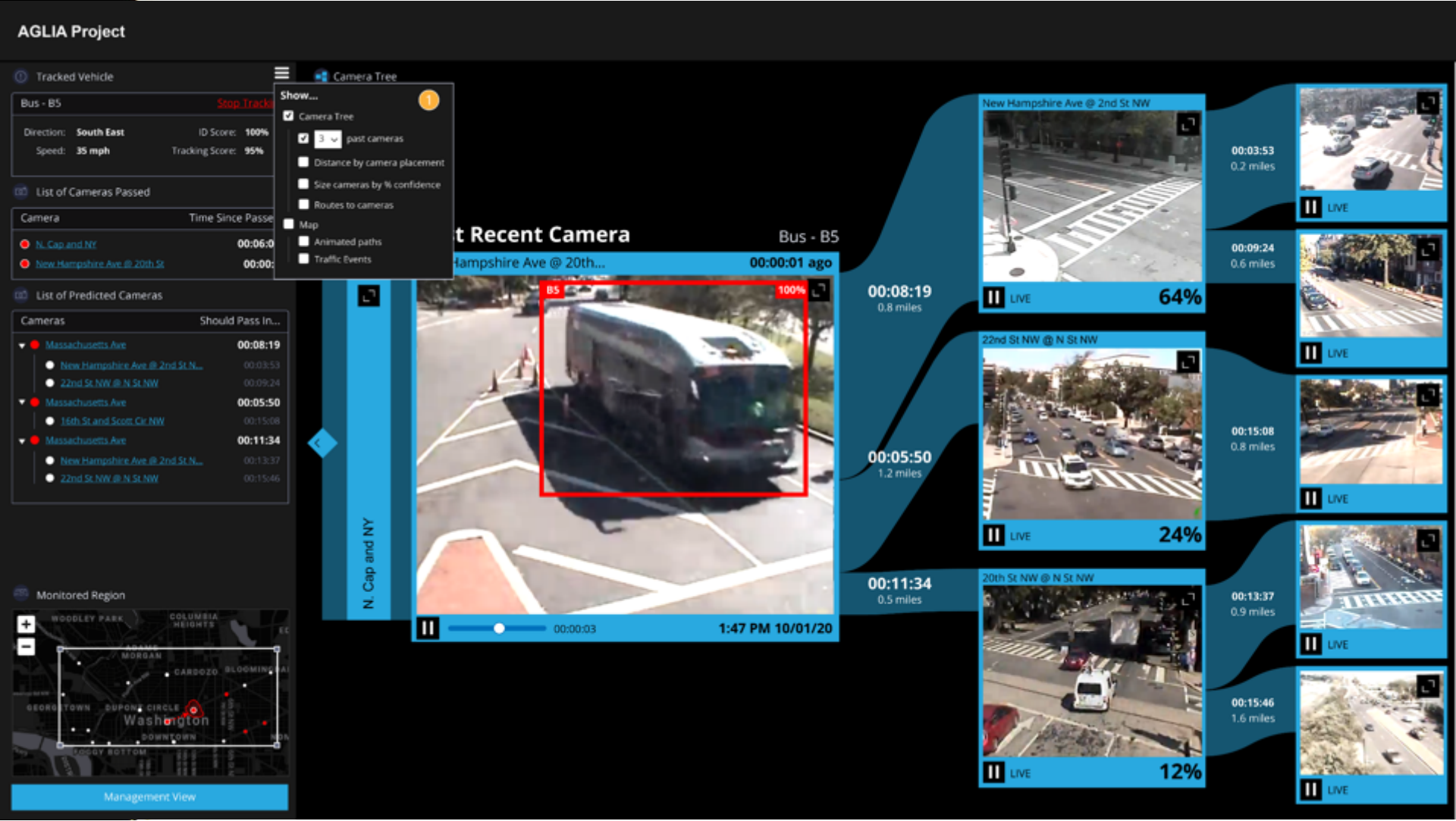

LIVE


LIVE


LIVE


LIVE


LIVE


AGLIA Project
Tracked Vehicle
Bus - B5
Stop Tracki
Direction: South East
ID Score: 100%
Speed: 35 mph
Tracking Score: 95%
List of Cameras Passed
Camera
Time Since Passe
N. Cap and NY
00:06:0
New Hampshire Ave @ 20th St
00:00:
List of Predicted Cameras
Cameras
Should Pass In...
Massachusetts Ave
00:08:19
New Hampshire Ave @ 2nd St N...
00:03:53
22nd St NW @ N St NW
00:09:24
Massachusetts Ave
00:05:50
16th St and Scott Cir NW
00:15:08
Massachusetts Ave
00:11:34
New Hampshire Ave @ 2nd St N...
00:13:37
22nd St NW @ N St NW
00:15:46
Monitored Region
WOODLEY PARK
COLUMBIA HEIGHTS
MORGAN
CARDOZO
GEORGETOWN
DUPONT CIRCLE
Washington
DOWNTOWN
FOGGY BOTTOM
Management View
Camera Tree
Show...
Camera Tree
past cameras
Distance by camera placement
Size cameras by % confidence
Routes to cameras
Map
Animated paths
Traffic Events
t Recent Camera
Bus - B5
Hampshire Ave @ 20th...
00:00:01 ago
B5
100%
N. Cap and NY
00:00:03
1:47 PM 10/01/20
00:08:19
0.8 miles
New Hampshire Ave @ 2nd St NW
LIVE
64%
00:05:50
1.2 miles
22nd St NW @ N St NW
LIVE
24%
00:11:34
0.5 miles
20th St NW @ N St NW
LIVE
12%
00:03:53
0.2 miles
LIVE
00:09:24
0.6 miles
LIVE
00:15:08
0.8 miles
LIVE
00:13:37
0.9 miles
LIVE
00:15:46
1.6 miles
LIVE

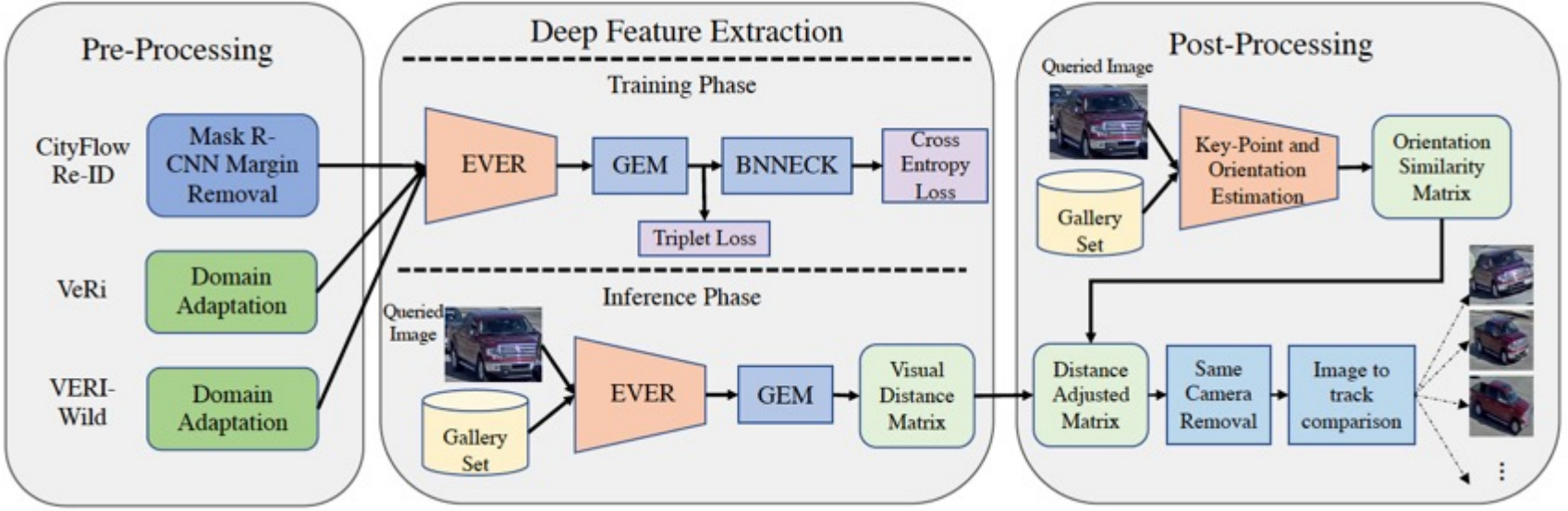
AGLIA Project

Fundamental research that produces tools for vehicle analytics and geolocation (GLIMPSE):

1. Vehicle detection, categorization, and labeling
2. Persistent tracking of moving objects
3. Anomaly detection
4. Language-based retrieval of vehicle retrieval
5. Geolocation of images and video that lack metadata (GLIMPSE)

City Scale Multi-Camera Vehicle Re-Identification

Vehicle Re-Identification is the task of locating all instances of a particular vehicle identity in a gallery set consisting of a large volume of vehicle images which have been captured under diverse conditions using a network of traffic cameras.



City Scale Multi-Camera Vehicle Re-Identification

- Pre-processing
  - Margin Removal
  - Domain Adaptation

(a) Original Image (b) Tightened

(a) Original Image (b) Mapped Image

- Deep Feature Extraction
  - Excited Vehicle Re-Identification with Generalized mean Pooling (GEM)
  - FASTREID Framework
  - Triplet + Cross Entropy Objective Functions

$$\mathcal{L}_t = \frac{1}{B}\sum_{i=1}^{B}\sum_{a\in b_i}\left[\gamma + \max_{p\in\mathcal{P}(a)}\|x_a - x_p\|_2 - \min_{n\in\mathcal{N}(a)}\|x_a - x_n\|_2\right]_+$$

$$\mathcal{L}_c = \frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{C}\left[y_j^i \log \hat{y}_j^i + (1-y_j^i)\log(1-\hat{y}_j^i)\right]$$

- Post-Processing
  - Same Camera Removal
  - Orientation Bias Removal
  - Image to Track Comparison

$$d(I_q, I_g) = \|f(I_q) - f(I_g)\|_2 + \lambda\frac{g(I_q).g(I_g)}{\|g(I_q)\|_2\|g(I_g)\|_2}$$

Peri, N, P. Khorramshahi, S. S. Rambhatla, V. Shenoy, S. Rawat, J.C. Chen, and R. Chellappa. "Towards real-time systems for vehicle re-identification, multi-camera tracking, and anomaly detection." In *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pp. 622-623. 2020.

He, L. X. Liao, W. Liu, X. Liu, P. Cheng, and T. Mei. "FastReID: a Pytorch toolbox for real-world person re-identification." *arXiv preprint arXiv:2006.02631*(2020).

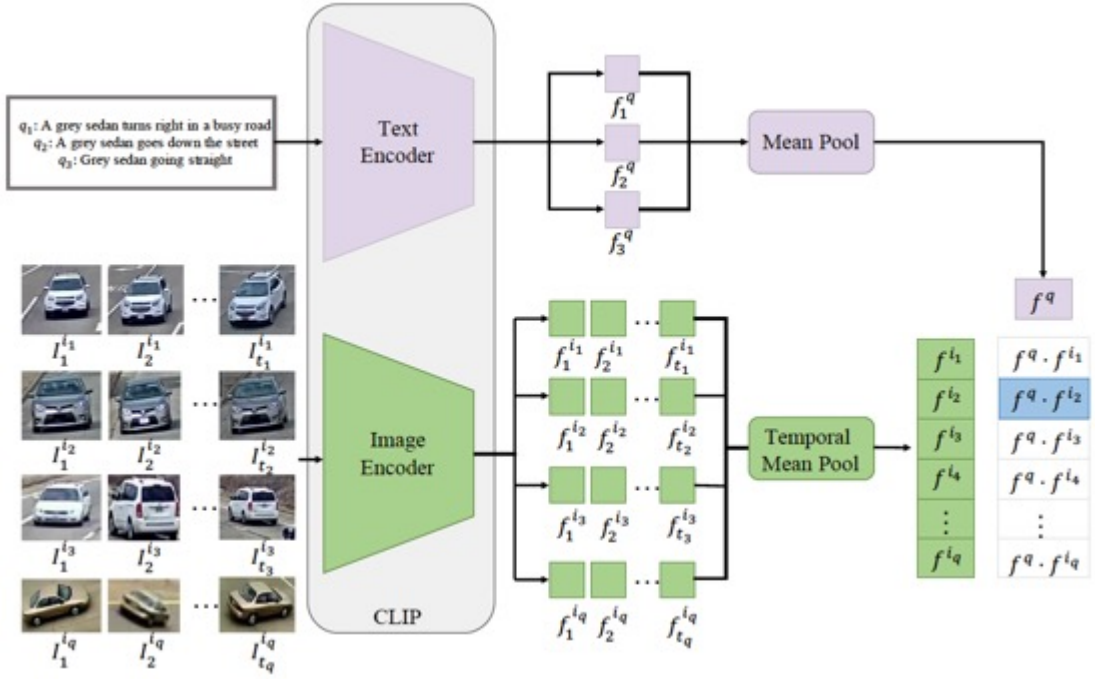
City Scale Multi-Camera Vehicle Re-Identification

- Evaluation Metric:
  - Mean Average Precision (mAP): mAP shows how well a gallery set can be ranked based on a given query set and higher values of this metric shows the superiority of the performance

Rank	Team Name	Score (mAP)
1	DMT	0.7445
2	NewGeneration	0.7151
3	CyberHu	0.6650
4	For Azeroth	0.6555
5	IDo	0.6373
6	KeepMoving	0.6364
7	MegVideo	0.6252
8	**aiem2021 (Ours)**	**0.6216**
9	CyberCoreAI	0.6134
10	Janus Wars	0.6083

Natural Language-Based Vehicle Retrieval

Natural Language-Based vehicle retrieval is a multimodal task for retrieving single-camera tracks of vehicles that are consistent with a natural language query describing its visual and motion patterns.



Radford, Alec, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry et al. "Learning transferable visual models from natural language supervision." *arXiv preprint arXiv:2103.00020* (2021).

Natural Language-Based Vehicle Retrieval

- Evaluation Metric:

  Mean Reciprocal Rank (MRR): Each individual query in the test set receives a score of the reciprocal of the rank at which the first correct response was returned. The value is zero if none of the five responses is the correct response.

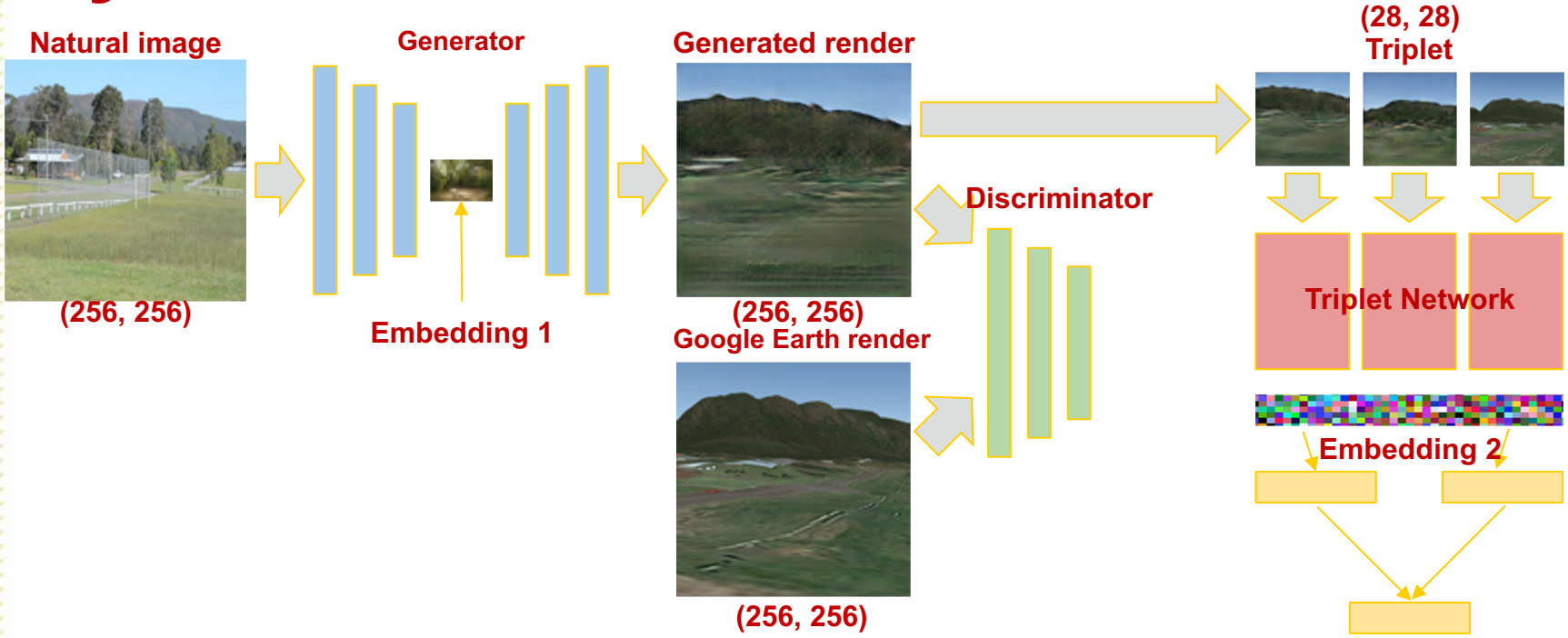
Rank	Team Name	Score (MRR)
1	Alibaba-UTS	0.1869
2	TimeLab	0.1613
3	SBUK	0.1594
4	SNLP	0.1571
5	HUST	0.1564
6	HCMUS	0.1560
7	VCA	0.1548
8	**aiem2021 (Ours)**	**0.1364**
9	Enablers	0.1314
10	Modulabs	0.1195

Machine learning for geolocation

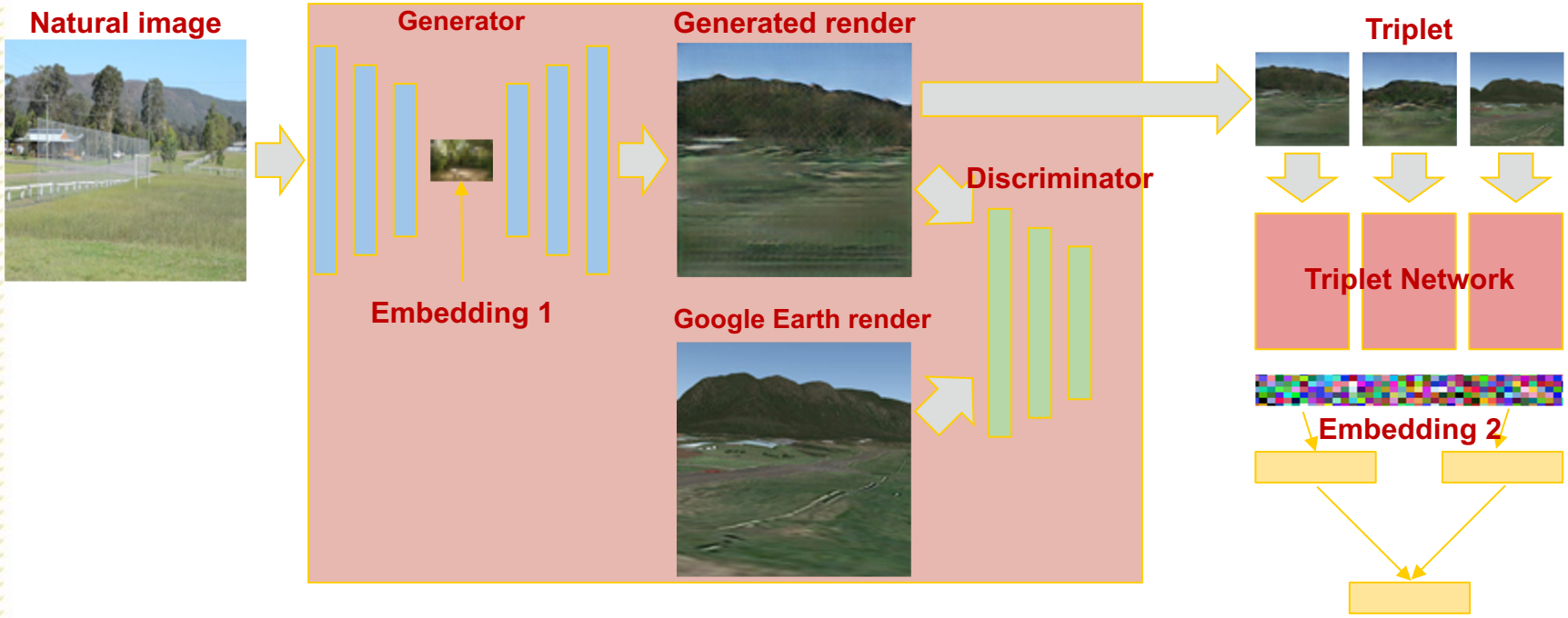
Completed GAN + triplet network system, using a modified pix2pix and a modified triplet network

Seeing an **improvement in accuracy, even though images are sized down** to 28 x 28 for faster training!

System overview

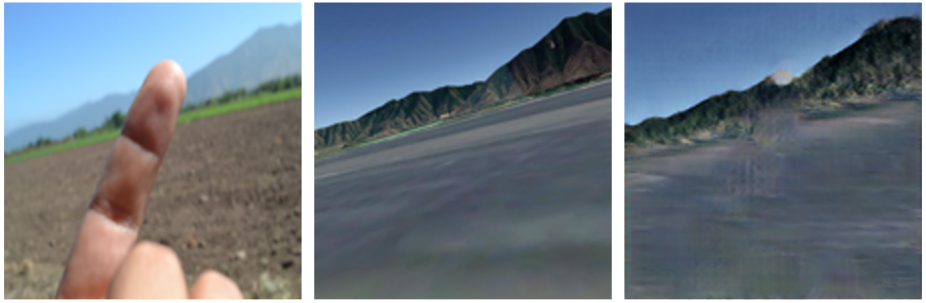


System overview

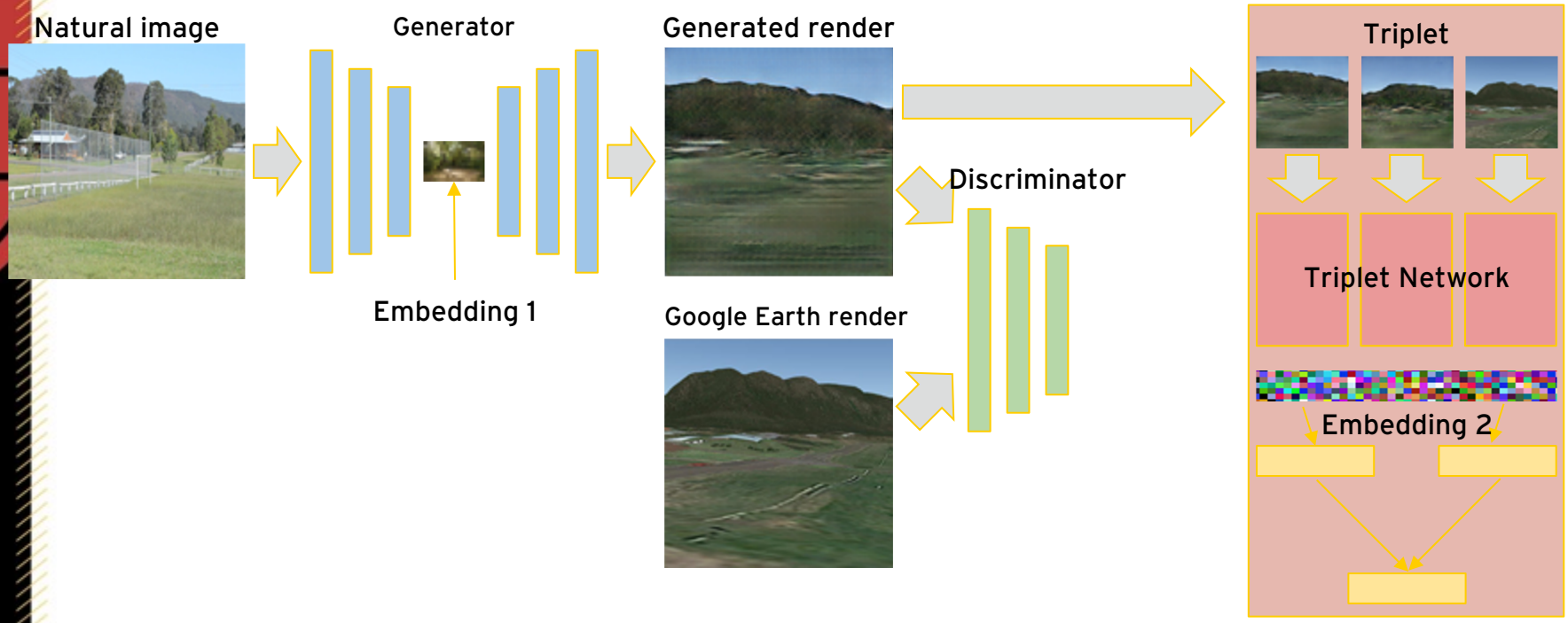


GAN

- Started off with pix2pix repository
- Generated images sufficiently recognizable when trained on ~150 locations (with at least one positive candidate each)!
- Tried to generate larger, higher resolution images with sub-networks at multiple scales, inspired by pix2pixHD

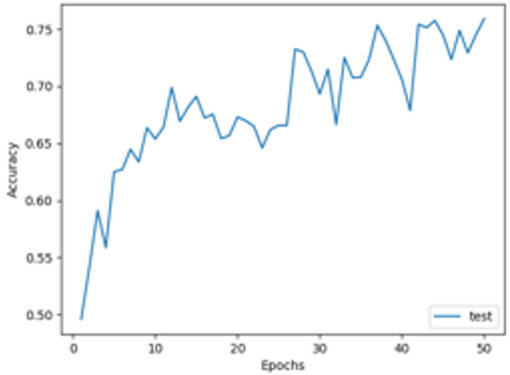


System overview



Triplet Network

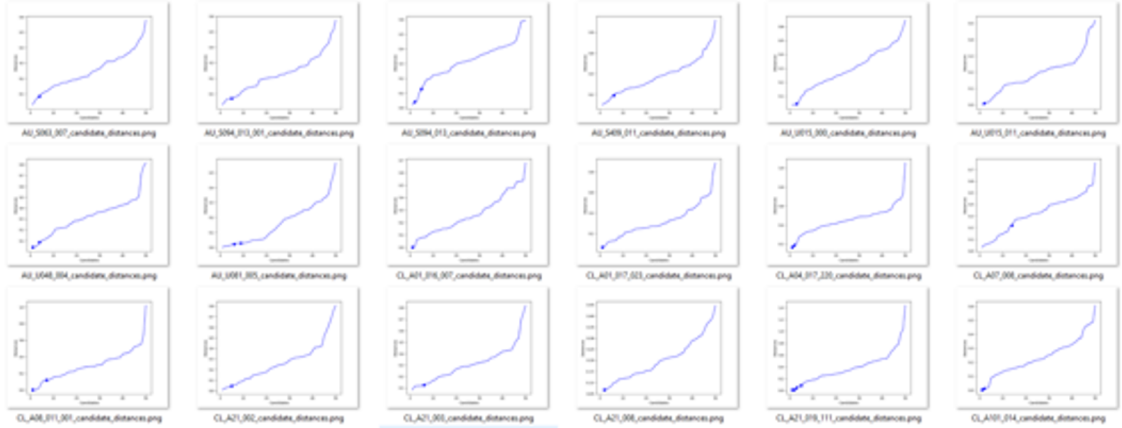
- Training off ~150 locations, 50 candidates each, results in 24523 triplets
- Takes a while to train, so currently using very small embedding networks again (images resized to 28 x 28).
- Trained multiple times on different subsets to determine accuracy of triplet network.



Results

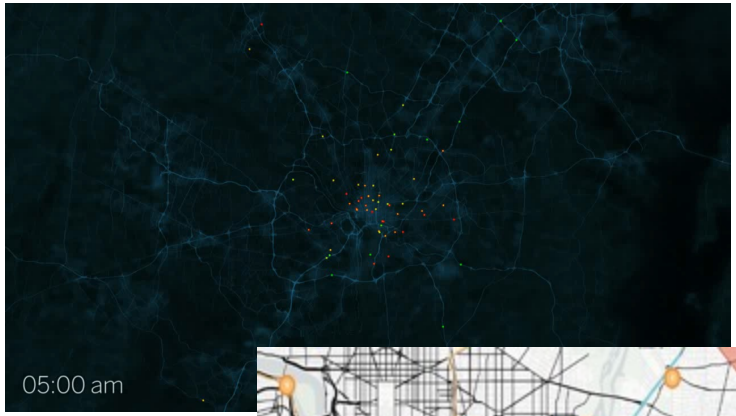
Accuracy
77.92
76.53
76.90
77.49
76.76
77.43
76.90
78.10
77.25

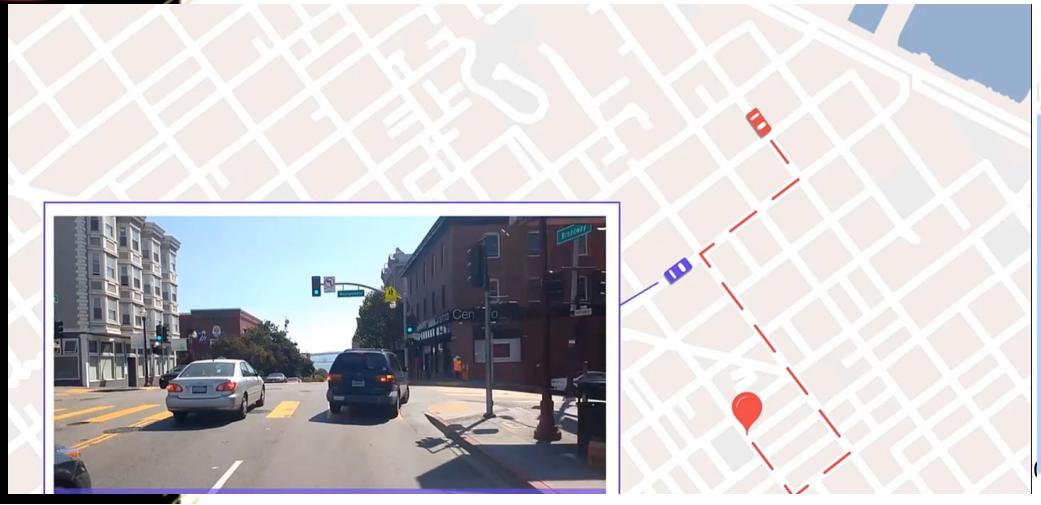
- **Improved accuracy** after adding generative step? Even after downsizing images, which in the past seemed to negatively impact accuracy
- Before was working with Google Earth renders; now the complete system works with the natural images and candidate location information
- **Next step:** size the embedding networks back up
- **Next step:** try another dataset?

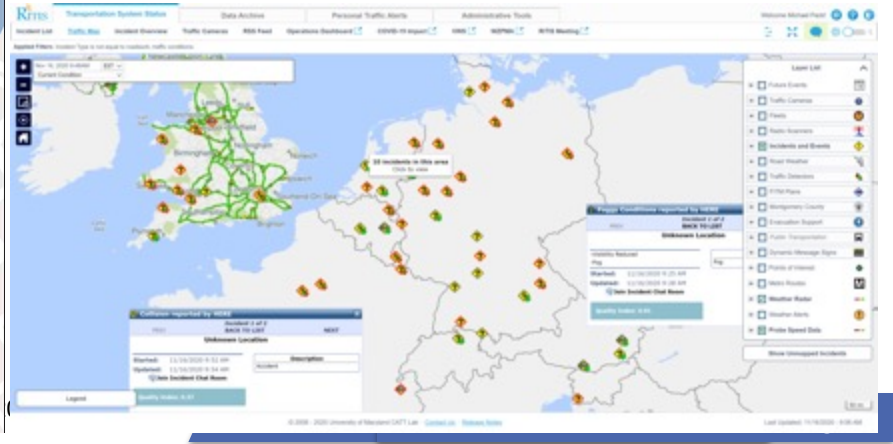


AGLIA Next Steps:

- Build-out of AGLIA Platform (in progress)
- Usability Testing
- Explore additional data for tracking capabilities
  - Images directly from private vehicles
  - Real-time trajectories (GM et al)
    - Signals in D.C.







Big Wins (for this project so far)

- Participation in 2020 and 2021 AICity Challenges
  - Natural language-based vehicle retrieval
- End-to-end systems based on deep learning foe vehicle analytics – under integration by CATT personnel
- Generative adversarial network (GAN)-based geolocation is showing promising results
- Publications in premier computer vision conferences and workshops (ICCV 2019, ECCV 2020, CVPR workshops 2020, 2021)

Thank you!

Michael L. Pack

PackML@umd.edu

Center for Advanced Transportation Technology Laboratory (CATT Lab)
University of Maryland

www.cattlab.umd.edu

www.ritis.org

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Autonomy Application and Engineering Exploratorium Phase 2 (A2E2)

Dr. Laurel G. Miller-Sims, Associate Research Scientist

lmillersims@arlis.umd.edu

Mission Area: Operationalizing Artificial Intelligence, Autonomy, and Augmentation (AAA)

- trusted evaluation partner on DARPA HIVE and SDH
- engaged in every step of the testing and evaluation life cycle
  - problem identification
  - dataset selection/generation
  - performance analysis
  - to scalable, reproducible benchmarking for trade-off aware comparative analysis.

Systems engineering
- Integrated system TEVV

Research and development
- Advancing TEVV for AI and autonomy

Relationship to ARLIS's goals/story

- Establishes ARLIS as a testbed for emerging AI technologies
- Leverages role of ARLIS as a Trusted Agent to facilitate transition of emerging hardware technologies to specific USG applications
- Engages UMD faculty and students in state of the art research on emerging AI hardware technologies with a focus on defense and intelligence applications.

Big Wins (so far)

Unclassified AI Testbed

- HIVE/Intel PIUMA emulator
- HIVE/Intel PIUMA simulator
- SDH/Hammerblade simulator

HIVE/SDH Transition Opportunities

- National Geospatial-Intelligence Agency Research (NGA-R)
- Secretary of the Air Force Concepts, Developments and Management (SAF/CDM)
- UMD Laboratory for Physical Sciences (LPS)
- USTRANSCOM Army Surface Deployment and Distribution Command (TRANSCOM SDDC)

Autonomy Application and Engineering Exploratorium Phase 2

- Sponsor: DARPA MTO
- Program Managers: Bryan Jacobs (HIVE)
  Ali Keshavarzi (SDH)
- Period of Performance: Oct20 - May21 (HIVE) *extension expected*
  Oct20 - Sep22 (SDH)
- TRL of the work: 4
- Total Budget: $2,473773 (HIVE) / $1,233,708 (SDH)
- Expenditures to date: $1,802,119 (HIVE) / $460,528 (SDH)

Team Members

- PI: Dr. William C. Regli
- ARLIS Team Members:
  - Dr. Laurel G. Miller-Sims (co-PI)
  - Jacob Bunker
  - Jared Ott
- Consultants/Subcontractors
  - Ben Johnson
  - Justin Gawrilow
  - Ezekiel Barnett

Major Subtasks

- Testbed for Emerging Hardware
- Assessment/Evaluation of Defense Applications for HIVE
  - Hierarchical Identify, Verify, Exploit
  - Graph analytics processing with 1000x efficiency
- Assessment/Evaluation of Defense Applications for SDH
  - Software Defined Hardware
  - Reconfigurable hardware/software optimized for data intensive applications with near ASIC efficiency

Project Description

Goal: *Enable and support specific HIVE and SDH transition opportunities*

SWOT: *Piecemeal as needed, difficult to compare across systems*

Expected Outcome: *Identification / implementation of specific USG use cases for HIVE and SDH hardware technologies in graph analytic, machine learning and data science pipelines*

Success measures: *Improved efficiency of USG transition partner workflows*

Expected Impact: *Enable the USG to leverage the unique efficiency and cost advantages of HIVE, SDH and future emerging hardware technologies on specific large-scale, data-intensive operational challenges*

A2E2 / Testbed Overview

Unclassified Testbed

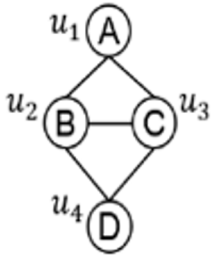
- HIVE / Intel PIUMA emulator
  - Dual motherboard, x8 FPGA
  - Emulates 2 cores with 4GB IPM
- HIVE / Intel PIUMA simulator
  - Theoretically, simmulates arbitrarily many cores
  - In practice, simulates up to 16 cores
- SDH / Hammerblade simulator
  - University of Washington SDH system

A2E2 / HIVE Transition Overview

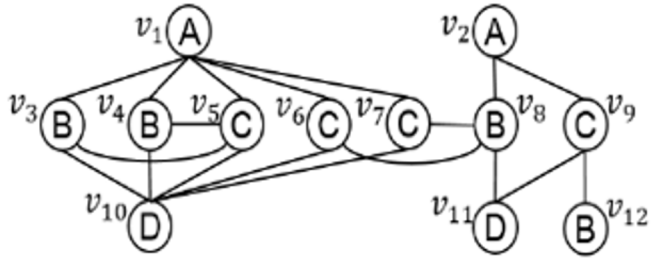
- NGA-R Graph Analytics
  - Use Case: <classified>
  - Technical Problems: graph matching, link prediction, node-labelling
- SAF/CDM GATR (Graph Analytics Test Resource)
  - Use Case: <classified>
  - Technical Problems: graph matching / subgraph isomorphism
- Graph Matching
  - Survey of Hardware Accelerated Graph Matching
  - PIUMA Implementations of Graph Matching Algorithms (UCLASM, FAQ, VF2)

A2E2 / Graph Matching

Problem: Given a small query graph q and a large world graph G, find all subgraphs of G that are isomorphic to q. That is, find an edge-preserving mapping of the nodes of q to a subset of the nodes of G.



(a) Query graph q



(b) Data graph G

A2E2 / Graph Matching

UCLASM / Overview

- Subgraph isomorphism algorithm developed under DARPA MAA
- Iterated filters + depth first search

  0) At initialization, all possible node mappings are candidate matches

  1) Repeatedly run series of filters to prune candidate matches

  2) When filters converge, make a provisional match between an unmatched query and world node.

  Go to 1)

A2E2 / Graph Matching

UCLASM / Topology Filter

Topology Filter

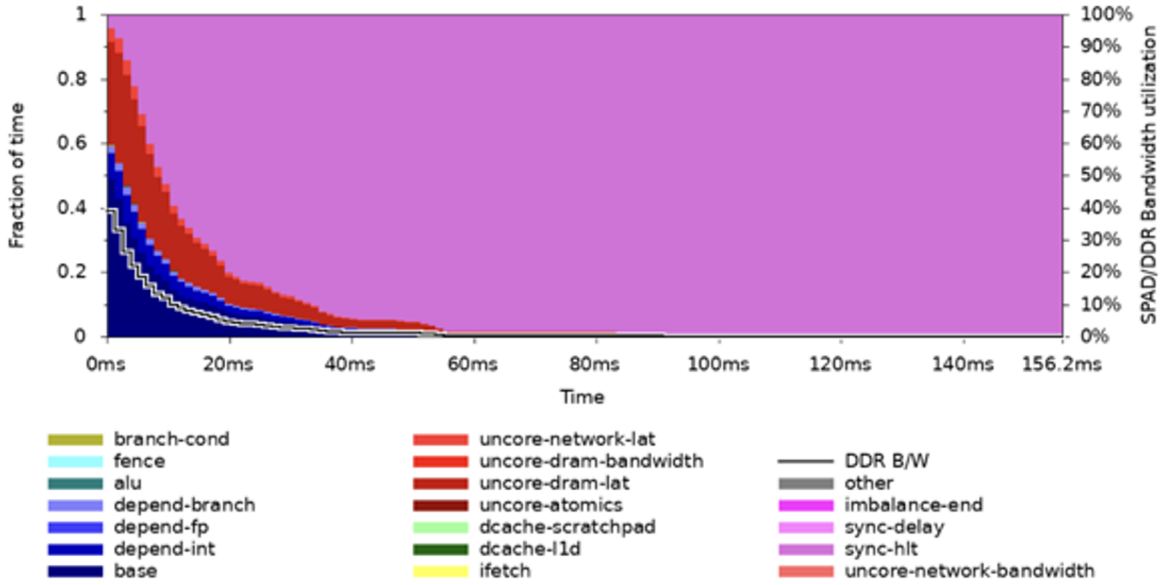
- Eliminates a candidate node mapping v->w if one of v's edges in the q is incompatible with all edges of w in G
- Major bottleneck in UCLASM pipeline
- Significant speedups from careful CPU implementa

	Stats Filter	Topology Filter	Permutation Filter
`python` (original)	7.47s	100.59s	32.2
`python` (`numba`)	3.87s (1.9x speedup)	1.63s (61x speedup)	0.76s (42x speedup)
`C++` & `OpenMP` (20 threads)	^	0.12s (838x speedup)	^

A2E2 / Graph Matching

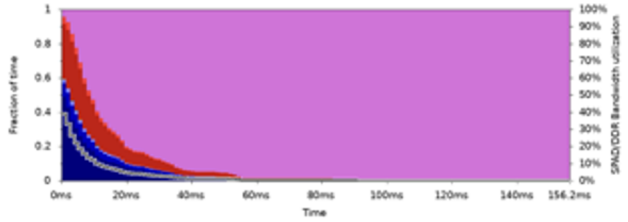
UCLASM / Topology Filter PIUMA Implementation

- Initial PIUMA implementation gives 768x speedup over optimized CPU implementation

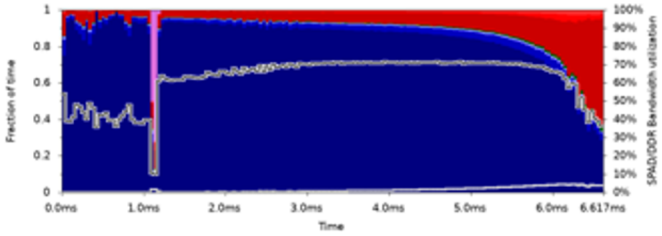


A2E2 / Graph Matching

UCLASM / Topology Filter PIUMA Implementation

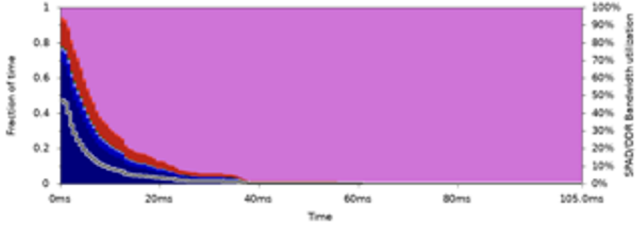


23.61x



enable caching
reduces latency

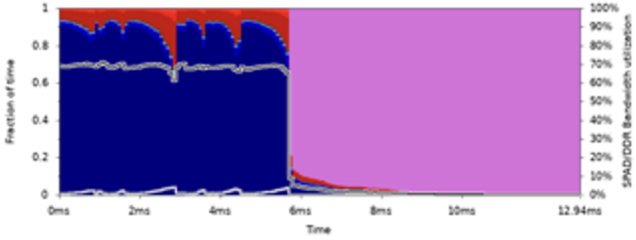
1.49x



parallelize expensive
computations to reduce
tail runtime

1.96x

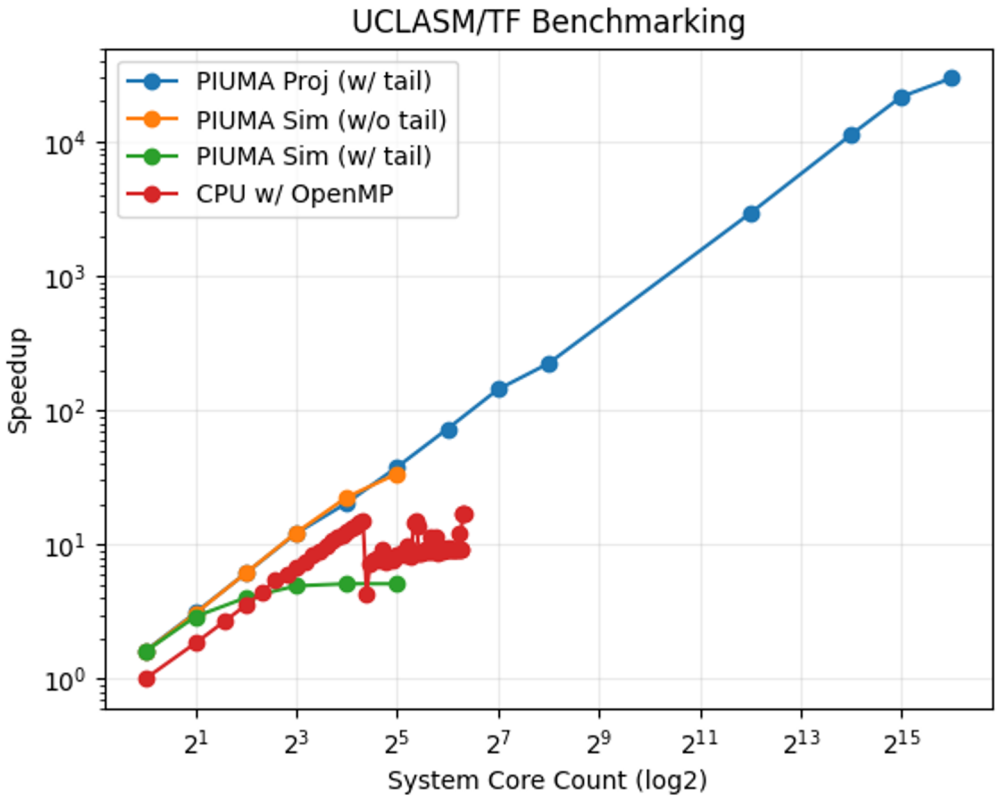
8.11x



dynamic scheduling
reduces load imbalance

A2E2 / Graph Matching

UCLASM / Topology Filter PIUMA Scaling



- Simulation matches projection well … if you ignore the “long tail”
- long tail caps performance.
- Next step (in progress): “two-branch” implementation that processes expensive nodes in parallel.

* PUMA Simulations > 4 die hang
* 0-20 CPU threads = 1 socket; > 20 threads 2 sockets; experiments on DARPA DGX-1

A2E2 / HIVE Transition Overview

- LPS
  - Use Case: <classified>
  - Problem: Breadth First Search, triangle counting, Jaccard, PageRank
- NGA-R GLIMPSE (Ground Level Image Processing SEgment)
  - Use Case: Automatic Geolocation of Imagery
  - Technical Problems: image classification
- USTRANSCOM SDDC
  - Use Case: large-scale logistics
  - Technical Problems: approximate optimization

A2E2 / SDH Transition Overview

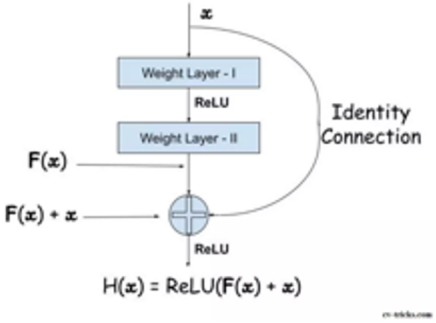
- Analytic Assessment of SDH Workflows
  - Identification of constituent kernels
  - Survey of existing applications to be leveraged on transition challenges
- Implementation / Optimization of SDH Workflows
  - CPU implementation of 4 SDH workflows with 10-1000x runtime improvements over existing benchmark implementations

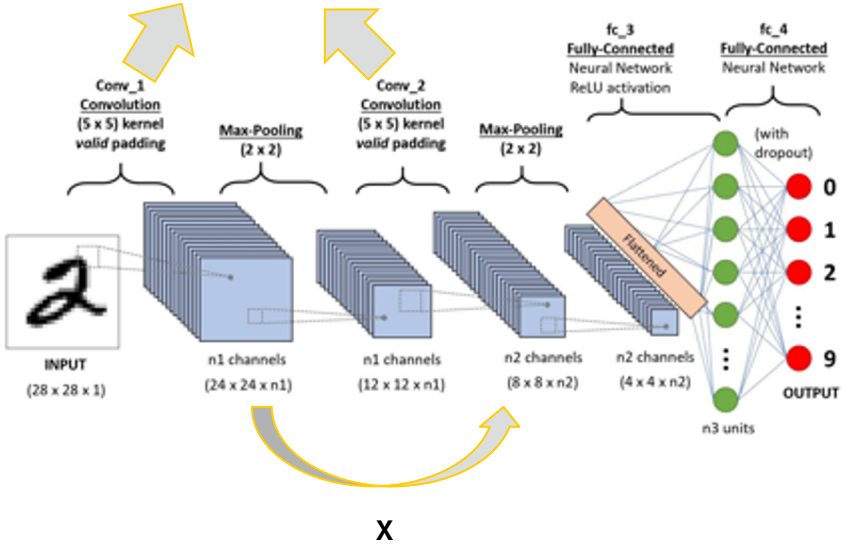
convnet is a residual network for image classification

- Convolutional Neural Networks (CNNs) successfully capture spatial and temporal dependencies in images/video
- Images are separated into channels
- Residual CNNs (ResNets) increase accuracy by reducing the impact of vanishing/exploding gradients.

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} * \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{m1} & y_{m2} & \cdots & y_{mn} \end{bmatrix} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{(m-i)(n-j)} y_{(1+i)(1+j)}$$

F(x)

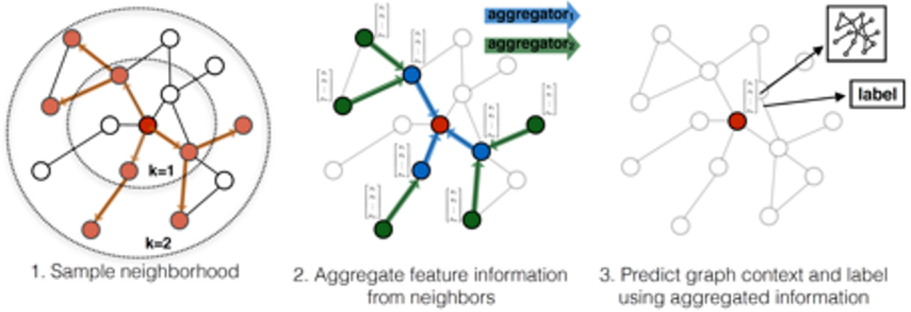


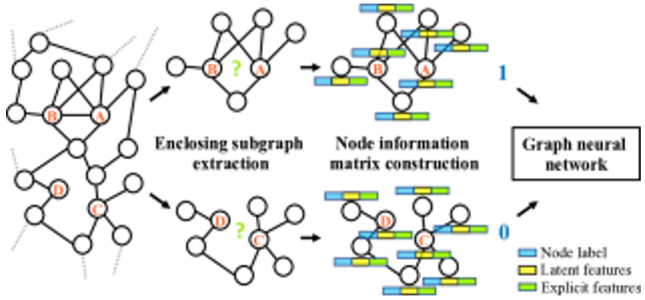


The identity or “skip” connections reuse upstream activations while layer weights are learned.

GraphSage is a framework for inductive representation learning on large graphs

- **learns low-dimensional representations for nodes**
- **encodes rich node attribute information**





SEAL Framework

- Extract local enclosing graph
- Use a GNN to learn graph features for link prediction

Link Prediction is a fundamental problem for network structured data

- knowledge graph completion
- recommender systems
- social network analysis

Given G, construct
- **G+, a training set of edges**
- **G-, a set of nonedges from G**

Score the edges in G+, G-
- **inner product / MLP /etc**

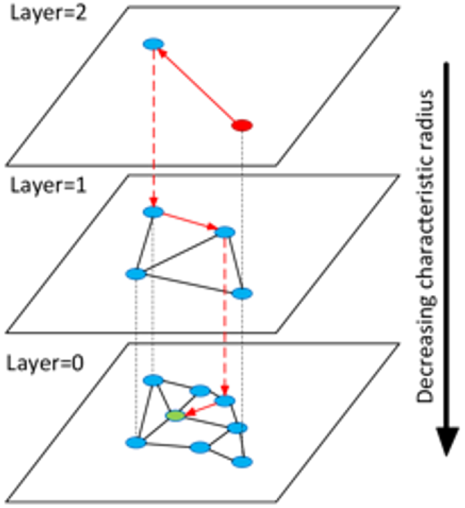
Train a GraphSage model on G
- **cross-entropy loss on scores**

ip-NSW is a graph-based retrieval algorithm that outputs approximate solutions to maximum inner product search (MIPS)

- inner product (i.e., cosine) similarity is a commonly used metric for comparing vectors
- used in recommender systems, natural language processing, computer vision

Indexing

1. create a hierarchical similarity graph
2. at each level add nodes iteratively
3. heuristically, link the added node to M similar nodes
4. acts as a series of filters for narrowing the pool candidate solutions



Query

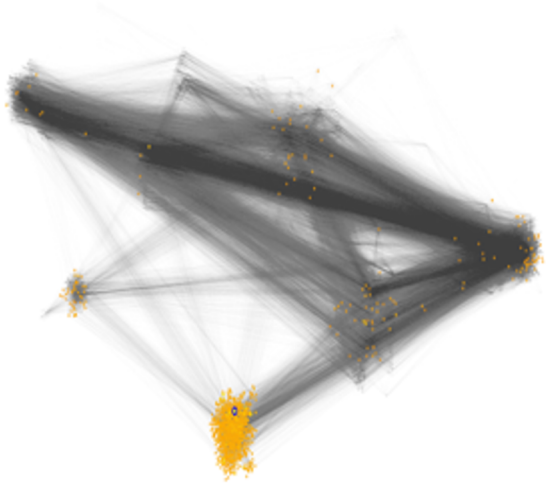
1. choose an entry point on top level
2. perform a greedy walk on the current level before descending
3. perform beam search on level 0 for a more robust search of remaining candidates

LGC: PageRank-Nibble & ISTA for L1-Regularized PageRank

- "Local graph clustering" (LGC) methods are approximate variants of personalized PageRank. Given a seed node in a network, the goal of LGC is to find a cluster of nodes that are "nearby" the seed.

PageRank-Nibble

- algorithm generates an approximate PageRank vector based on repeatedly pushing mass from vertices that have enough residual. A sweep cut is applied to the resulting vector to give a partition.

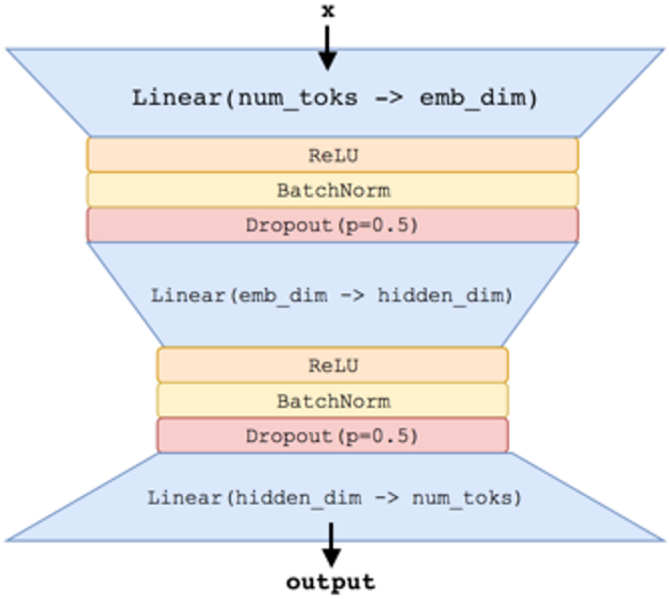


ISTA for L1-Regularized PageRank

- frames PageRank as an optimization problem and then applies a version of the iterative shrinkage-threshold algorithm (proximal gradient descent) to solve it.

Recsys (Autoencoder-based Recommender System)

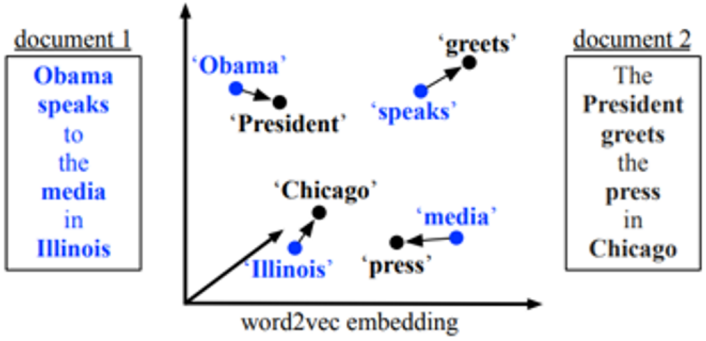
- An autoencoder that takes a list of items that a person has "liked", and predicts a score for all items.
- Autoencoders are neural network models where the input and the target are the same. By mapping the input through a lower dimension, we prevent the model from learning the identity function and force it to learn something about the structure of the data.

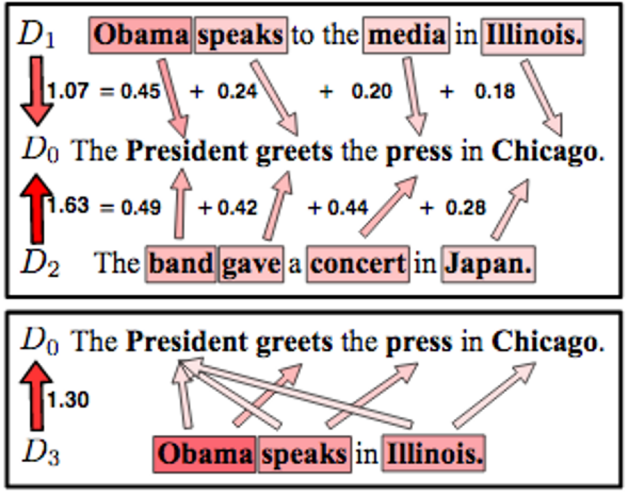


examples: NVIDIA DeepRec, AutoRec

Sinkhorn Word Movers Distance

- measures the distance or dissimilarity between two text documents.
  - Given documents A and B, generate d-dimensional vector representations of each word
  - Word Mover's Distance is the minimum cumulative distance needed for all words in A to the words in B

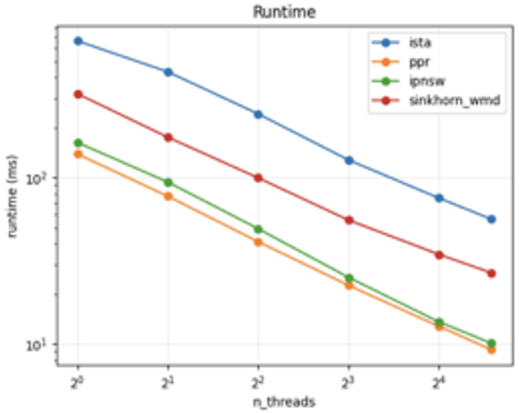


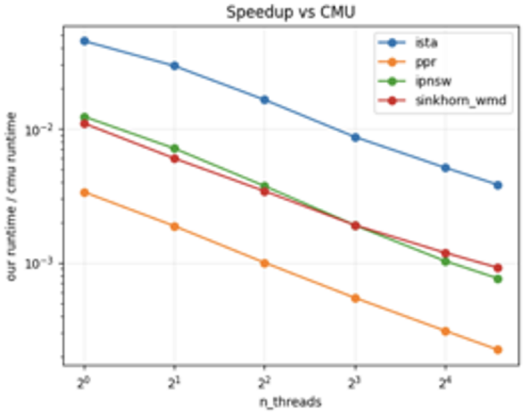


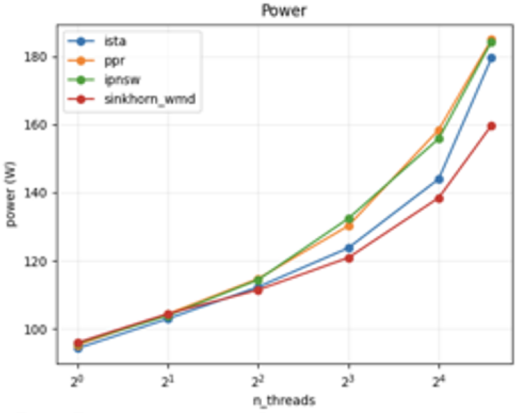
A2E2 / SDH Applications Overview

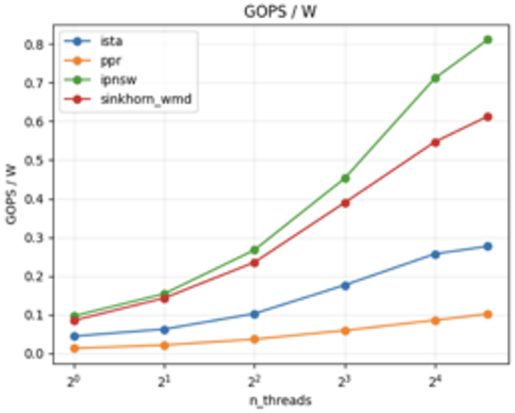
SDH Workload	Description	Application Example
convnet	CNN for image classification	image processing systems, facial recognition
graphsage	Representation learning on large graphs	predict target associations
ip-NSW	Graph-based retrieval	identify similar targets in a social network
PR-Nibble **ISTA**	Local graph clustering	find targets with similar patterns of communication
Recsys	Recommender system	target recommendation
Sinkhorn Word Mover's Distance	Text similarity metric	Social media text comparison

A2E2 / SDH Workload Optimization









- implemented in C/C++/OpenMP
- oprimized for runtime
- Optimizations
  - op reduction
  - different data structures
  - avoiding unnecessary computation

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
SCI-Accredited AI Testbed	June 2021	Delayed
Transition Use Case Studies	August 2021	On Sched
Graph Matching Report	August 2021	On Sched

Project Risk Assessment

- Security/IP barriers to obtaining transition partner data/code.
- SCI-accreditation of testbed delayed due to COVID-19
- Mitigation: abstract analysis of surrogate workflows

Next Steps and Future Capabilities

- SCI-accredited Testbed
- Transition Use Case Experiments
  - NGA-R, LPS, SAF/CDM, TRANSCOM, LPS
- Identify Additional Transition Partners / Problems
  - Project MAVEN, DHS RAVEN
- Report: State of the Art for Hardware Acceleration of the Subgraph Isomorphism Problem

Thank you!

Laurel G. Miller-Sims, Ph.D.

lmillersims@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Integrated Discovery of Emerging and Novel Technologies (IDENT)

Steve Sin, Investigator/ PI (START)
Michael Maxwell, Research Scientist (ARLIS lead)
mmaxwell@umd.edu

Integrated Discovery of Emerging and Novel Technologies (IDENT)

- Sponsor: Defense Threat Reduction Agency (DTRA)
- Program Manager/Client: Reed Grabowski
- Period of Performance: 21 Jul 2020—20 Apr 2021
  (+ NCE requested by START)
- TRL of the work: 3-4
- Total Budget: $343,627 (VAC about +$12,000)
- Team Members:
  - ARLIS: M Maxwell, L Miller-Sims, (N Silbert), J Hull, D Peskov (N Adams)
  - START is lead (S Sin PI)
  - ABS Consulting (under START)

Project Description

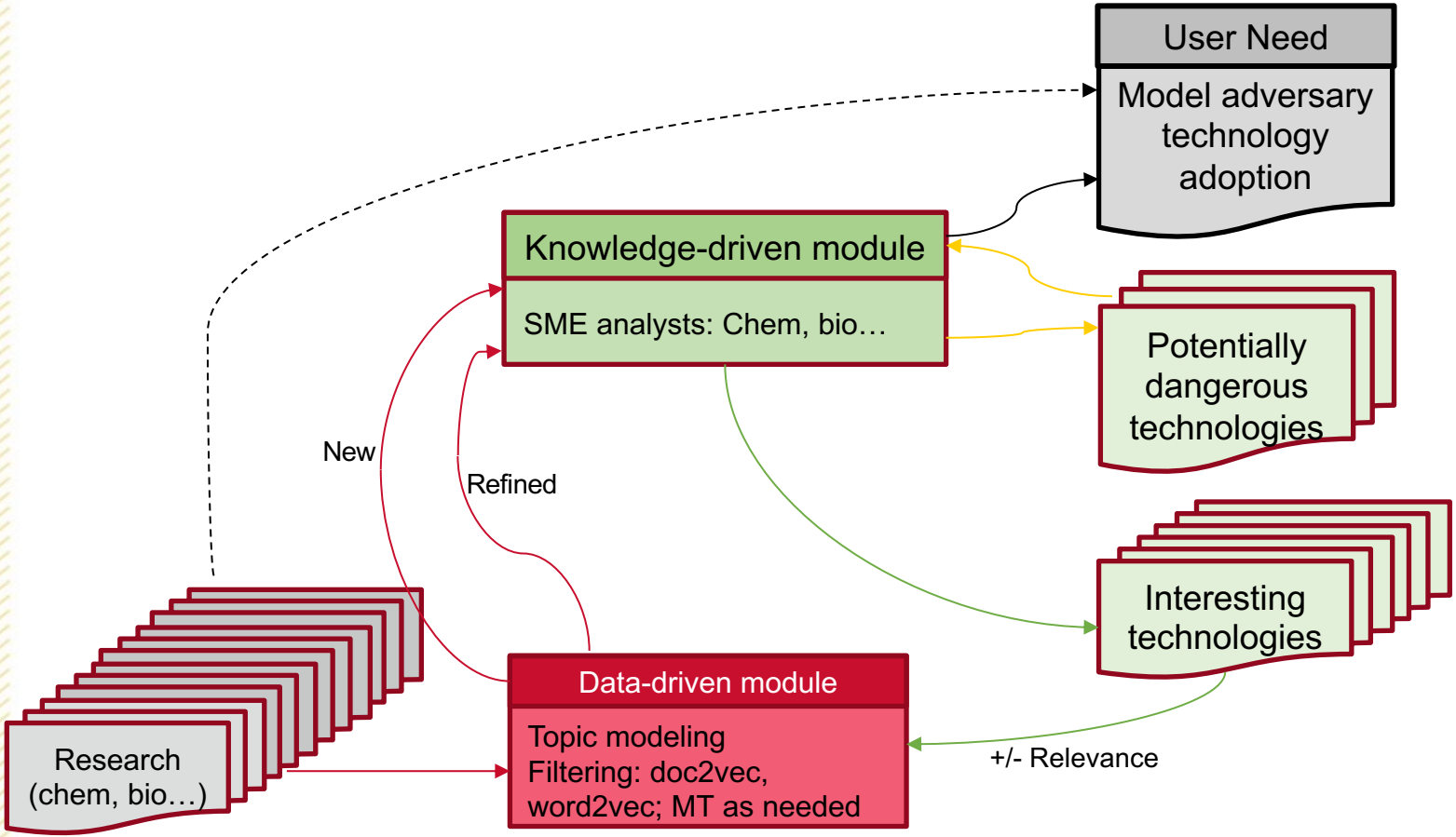
Goal: Enable IARPA to discover new technologies which adversaries might adapt for WMD (chemical, biological, radiological…).
ARLIS' role: Topic tracking, corpus search for related papers, pre-processing of data in multiple languages

SWOT: Analysts use existing generic search methods to keep up with open research.
Strengths: Analysts have domain expertise (SMEs)
Weaknesses: Volume, velocity; needle in haystack

Expected Outcome: USG gains ability to use human-in-the-loop automated search to monitor research outlets for developments of potential relevance to WMD, using machine translation for foreign languages.

Success measures: Testing has been done on very large corpora (by ARLIS) and web search (by ABS Consulting) using SMEs to filter and validate results (by START).

Expected Impact: DTRA to set up system on their classified network and use it to track potential new WMD threats.


User Need
Model adversary technology adoption
Knowledge-driven module
SME analysts: Chem, bio…
Potentially dangerous technologies
New
Refined
Interesting technologies
Research (chem, bio…)
Data-driven module
Topic modeling
Filtering: doc2vec, word2vec; MT as needed
+/- Relevance

Relationship to ARLIS's goals

- Human domain
  - "Our" humans: SMEs/ analysts in WMD
  - "Opponents": Terrorists, smaller nations
    Biological weapons = "the poor man's atomic bomb" (—Hashemi Rafsanjani)
- Relationship to other projects at ARLIS
  - ML for decision support (AAA)
  - Built on previous work with language processing
  - Added expertise in topic modeling (now used in several other projects)
    - Utility of linguistic pre-processing (English, French, Russian, Chinese)
    - Topic visualization
    - Usefulness of other language processing tools (BERT)
- Leverage our hybrid role
  - Joint venture between START and ARLIS (+ outside contractor)

Wins

- Explored metrics for evaluation of topics
- Unexpected finding: Non-stability of topics
  - With both medium and large corpora
  - Setting a fixed seed results in stability (but that's a kludge)
- Solution looking for problems: semantic modeling
  Useful for building lexicons of semantically related words in highly technical vocabulary:
  - dlbcl,lbl,bcl,lymphoma,b症状,ldh,国际预后指数,bcl2,p53,67指数
  - dlbcl, lbl, bcc, lymphoma, b-symptom, ldh, international prognosis index, bcl2, p53, [Ki-]67-index
- Transition
  - DTRA is receiving software + documentation + technical reports

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Software + documentation	Delivered 20 Apr	Completed on schedule
TR: Adding another language (Chinese)	Delivered 30 Apr	Completed on schedule

Project Risk Assessment

- Performing code review of archiving software for security issues
- NCE will allow response to any issues raised by USG
- No significant impact from COVID-19
  - Meetings held on Zoom rather than face-to-face
  - Denis Peskov was stuck in Germany, which slightly impeded code and data exchange

Next Steps and Future Capabilities

- Project is substantially complete, pending any issues raised by USG
- Potential conference paper on topic model stability
- Future:
  - Topic Modeling
    - Contact with MITRE re topic modeling (Jared Mowery, 23 Apr)
  - Semantic modeling of word meaning may have applications for language analysts, particularly in technical domains
    - White paper to Cyber SLA (9 Apr)

Thank you!

Mike Maxwell, Research Scientist

mmaxwell@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

There is No AI in Teams: A Multidisciplinary Framework of Features for AIs to Work in Human Teams

Dr. Susannah Paletz, College of Information Studies

paletz@umd.edu

There is No AI in Teams: A Multidisciplinary Framework of Features for AIs to Work in Human Teams

- Sponsor: ARLIS internal funds
- Program Manager/Client: ARLIS Leadership
- Period of Performance: May 24 – October 31, 2020
- Funding by USG FY: UMD FY2020 $49,980
- Funding type: 6.1
- TRL of the work: 1
- Team Members:
  - Dr. Susannah Paletz, College of Information Studies
  - ARLIS: Drs. Susan Campbell, Breana Carter-Browne, Craig Lawrence, Polly O'Rourke, Brian Pierce, Jana Schwartz
  - College of Information Studies PhD students: Melissa Carraway, Sarah Vahlkamp

Project Description

AI is an important part of the ARLIS portfolio; ARLIS brings multidisciplinary social science to problems and solutions.

Goal: Develop multidisciplinary framework for AIs to successfully serve/work within human teams. Also, define requirements and identify at least two gaps in current knowledge

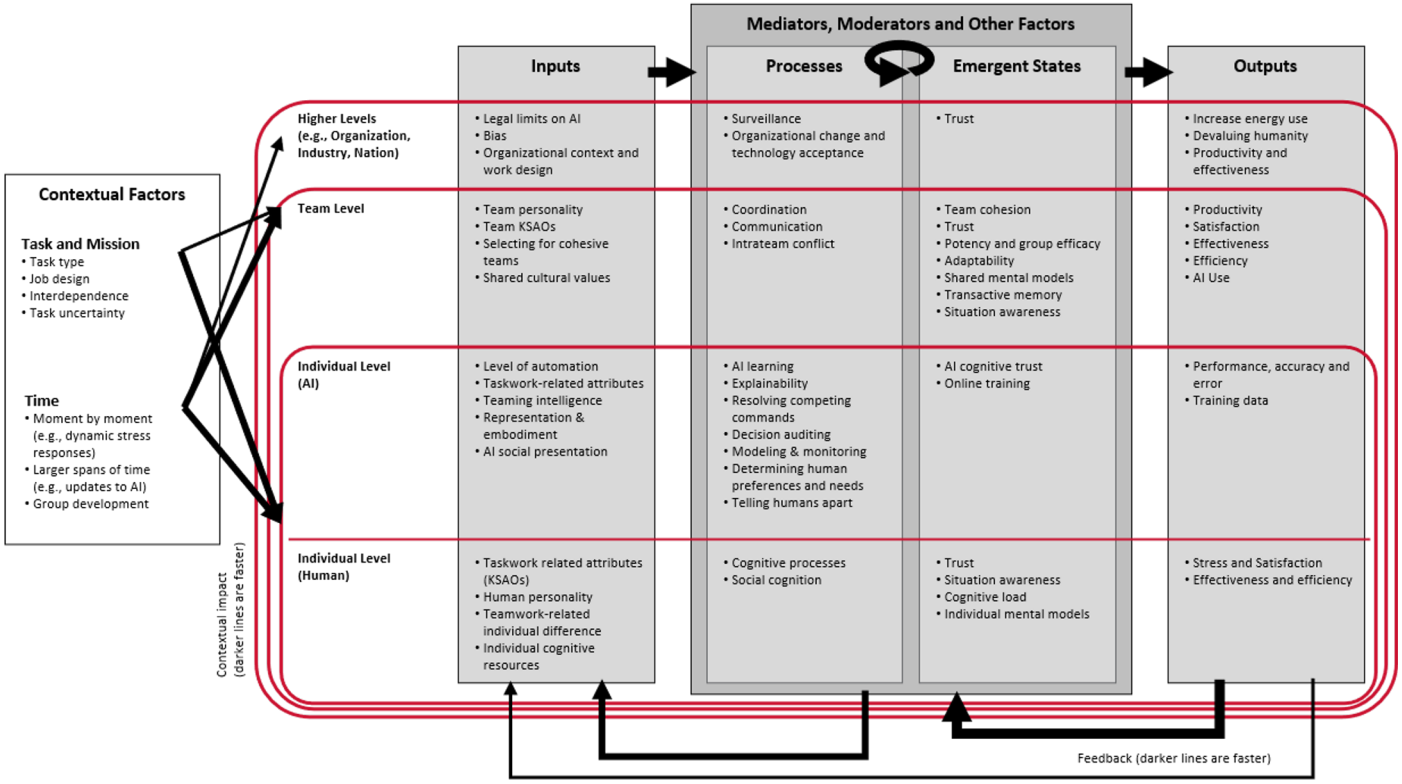
Expected Impact: Foundational work to inform design of AIs to collaborate as teammates within the human teaming system.

Success measures: Thorough framework that identifies requirements; gaps that ARLIS researchers can fill; potential clients; actual users of the frameworks; citations (eventually).

There is No AI in Teams Overview

- **Framework** created, extensive synthesized theory paper written
  - Levels: Individual Human, Individual AI, Team, Higher Levels (Organization, Industry, Society, etc.)
  - Factors/dimensions: Inputs, Processes (Mediators, Emergent States), Outputs
  - Contextual factors: Task and Mission, Time
- **Gaps/issues** in existing practice/literature: So many!
  - Many teamwork constructs not yet applied to AI
  - AI issues not yet considered at team or higher levels (e.g., explainability)
  - Organizational/societal constructs sparse, but important
  - Trust is a key, contested, complex issue across levels
  - Can AI be a teammate?
  - etc.

There is No AI in Teams Overview



Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Plan	April 2020	Complete
Collect literature, read, synthesize; lit sprint	May-August 2020	Complete
Gap analysis/identification; requirements	July-December 2020	High level in report
Create framework, write up	July-September 2020	Complete
Internal review	August-September 2020	Delayed
Deliver report (deadline #1)	October 2020	Delayed
Deliver report (deadline #2)	May 2021	In process

Project Status and Next Steps

- **Big Wins (so far)**
  - Completed model, exhaustive paper
  - Submitted extended abstract to 1 conference
  - Conversations with Jiangyin Zhou, Joshua Elliot, John Pashkewitz (DARPA), Alonso Vera (NASA)
  - Dr. Campbell presented at UMD HCIL group
  - Model informed models used in AAA program and SANDS2 project (presented elsewhere in this Program Review)
  - Drs. Lawrence and Campbell received funding from the Army Research Laboratory (ARL) as part of the 5-year UMD/UMBC AI and Automation in Multi-Agent Systems (ArtIAMAS) project to investigate “Human machine teaming and effective aggregation of information in complex systems”

Project Status and Next Steps

- **Transition goals/obstacles**
  - Goals: change conversation about AI and teams; grow ARLIS reputation; dissemination (smaller pieces) to conferences, journals, program officers, AI researchers, professors
  - Challenges: ARLIS internal reviews - how best to do?; finding funders interested in truly multidisciplinary work; personnel support to see papers to submission and resubmission
- **New ideas and whitepapers**
  - More theory: link sociotechnical studies, psychology, management, AI/CS
  - Spin-off empirical studies
  - Inform AI, human-machine teaming work at ARLIS, DARPA, NSF, ARO
- **Sponsor relationship, new/additional sponsors**
  - Find external funding: potential end-users include AI creators (e.g., US Cyber Command, services)

Thank you!

Susannah Paletz

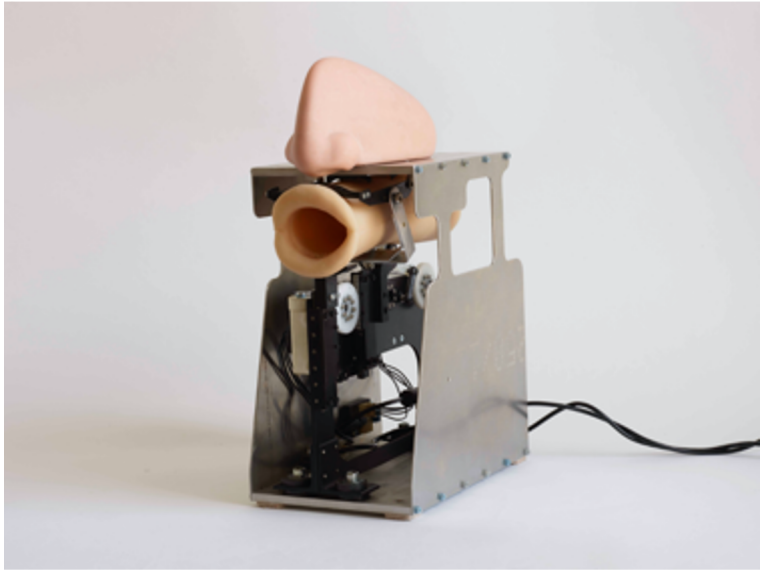
paletz@umd.edu

College of Information Studies

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Functional requirements: met
Implicit requirements: met?



THE PRAYER

or

An experimental set-up to explore the possibilities of an approximation to celestial and numinous entities by performing a potentially never-ending chain of religious routines and devotional attempts for communication through a self-learning software.

Diemut Strebe https://theprayer.diemutstrebe.com

Human Performance: Augmentation

Focus Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

DARPA Targeted Neuroplasticity Training (TNT)

Polly O'Rourke, Associate Research Scientist

porourke@arlis.umd.edu

DARPA TNT

- **Sponsor:** DARPA BTO
- **Program Manager/Client:** Tristan McClure-Begley
- **Period of Performance:** 4/17/17 – 12/17/21
- **Total Budget (+ Expenditures to Date):** $7.96M ($7.19M)
- **TRL of the work:** 1

DARPA TNT Team Members

- PI Polly O'Rourke, Co-PI Stefanie Kuchinsky, Co-PI Shihab Shamma
- Team Members:
  - **ARLIS**
    Postdocs: Regina Calloway, Michael Johns, David Martinez, Ian Phillips
    FRSs: Val Karuzis, Sara McConnell, Nick Pandža, Alison Tseng
    GA: Meghan Hersh (SLA)
    Software Engineer: Jarrett Lee

  - **ISR:**
    Postdocs: Ali Mohammed, Daniel Stoltzberg

Shout out to Chris Gardner, Bret Howard, Monique Anderson, Joe Smith, Jackie Madoo, Erin Fitzgerald, Janelle Gabriel and Brian Shoemaker.

Project Description

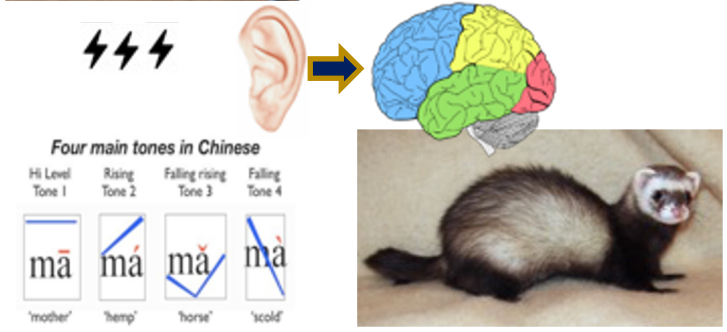
Goal:

- Evaluate auricular transcutaneous vagus nerve stimulation (taVNS) as a method of accelerating language learning.
- Examine impacts on vocabulary, grammar and tone learning.
- Evaluate additional nerve targets: trigeminal (tTNS) and cervical vagus (tcVNS)
- Conduct field study with USAF 517th Training Group in Monterey, CA (co-leading with AFRL and IHMC)
- Examine underlying mechanisms in animal studies.

Expected Impact: Validation of technique for improving military language training and cognitive performance generally.

Success measures: Significant enhancements in lab and field testing; tightly controlled, double-blind experiments.

DARPA TNT Overview



Project objectives

- Evaluate taVNS for vocabulary, grammar, tone learning and field study.
- Evaluate tcVNS and tTNS for grammar learning.
- Evaluate underlying mechanisms of vagus nerve stimulation through animal research.

Project status

- NCE extending PoP to 12/17/21.
- In-person data collection was delayed 1 year due to Covid19.
- Remote data collection for vocabulary / grammar study starting in May 2021.
- In person data collection for all lab experiments starting in August 2021.
- Field testing and animal research are ongoing.

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Resume data collection in all experiments	8/17/21	On sched
Complete data collection in all experiments	12/1/21	On sched
Final technical reports	12/17/21	On sched

- **Big Wins (so far)**: Promising effects; selected for option phase; $1M plus-up; NCE granted
- **Transition goals/obstacles**: Transition with USAF 517th and possibly with DLIFLC more broadly.
- **New ideas and whitepapers**: tVNS for cognitive bias; physiological markers of vagus stimulation; tVNS for TBI recovery.
- **Sponsor relationship, new/additional sponsors**: TBD

Thank you!

Polly O'Rourke

porourke@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Examining the Cognitive Underpinnings of Creativity

David Martinez, Research Associate

Dmartinez@arlis.umd.edu

Creative Problem-Solving

- Sponsor: ONR
- Program Manager/Client: LCDR Jacob Norris
- Period of Performance: 03/05/21–03/04/24
- Total Budget (+ Expenditures to Date): $607,736 (~$4000)
- TRL of the work: 1
- Team Members (co-pis, subawardees):
  - Polly O'Rourke

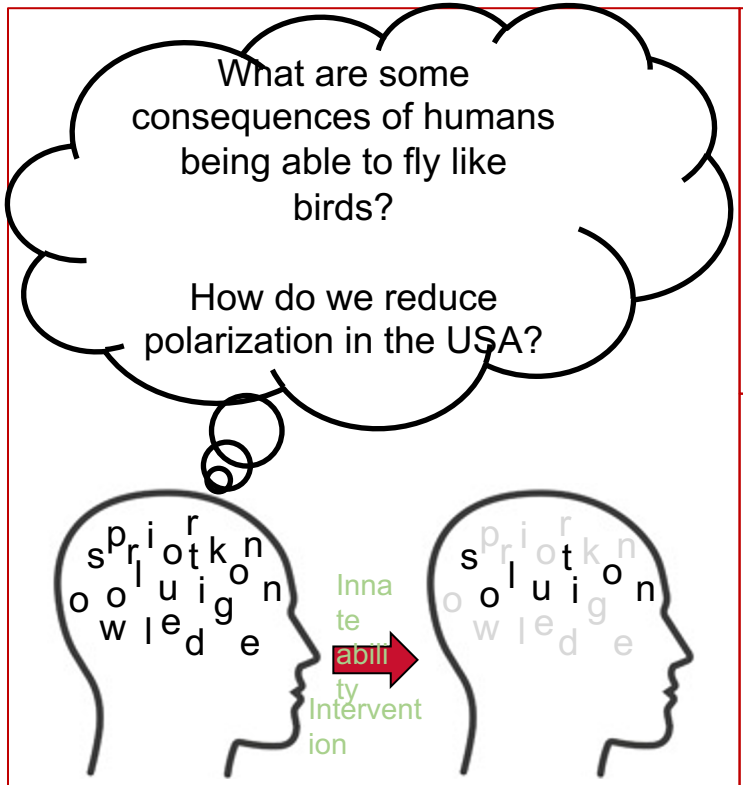
Project Description

Goal: Improve our understanding and assessment of creative problem solving and decision making

Expected Impact: selection tools; training programs and technologies to improve creative thinking; more creative and human-like AI.

Success measures: reliable and valid measures of creative thinking and decision making; statistically significant results supporting theory; dissemination of results in high-impact journals; continued funding.

Creative Problem-Solving Overview



Project objectives

- Identify and validate tests
- Improve creative thinking
- Identify a source of cognitive biases and suggest how to mitigate

Project status

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Kick-off	Complete	On sched
Test development	Ongoing	On sched
Recruiting staff (FRS and URAs)	Ongoing	On sched

- **Big Wins (so far)**: Successful kickoff!
- **Transition goals/obstacles**: Move to TRL 2/3
- **New ideas and whitepapers**: Creativity in learning
- **Sponsor relationship, new/additional sponsors**: TBD

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

Unbiasing Analysts:
Reducing Cognitive Biases in Intelligence Analysts with Non-Invasive Peripheral Nerve Stimulation

David Martinez, Research Associate

dmartinez@arlis.umd.edu

Unbiasing Analysts

- **Sponsor:** IRAD
- Program Manager/Client: **ARLIS**
- **Period of Performance:** June 2020 – October 2021
- **Total Budget (+ Expenditures to Date):** $52,590 ($9,836)
- **TRL of the work:** 1
- **Team Members:**
  - PI: Polly O'Rourke
  - David Martinez, Alison Tseng, Valerie Karuzis, Meghan Hersh

Project Description

Goal: Develop an inexpensive, user-friendly technique for increasing the effectiveness of intelligence analysts to detect and assess threats to national security.

Expected Impact: Reduce bias in intelligence analysts in order to prevent intelligence failures and increase effectiveness of analysis.

Success measures: Significant reductions in bias resulting from tVNS

Unbiasing Analysts Overview

Project objectives

- Reduce bias

Project status

- Officially began 01/2021
- To continue through Summer 2021

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
IRB application	Submitted	On time
Test Development	Completed	On time
Field Testing	Dropped	Issue

- **Big Wins (so far)**: summer staff; development of analyst relevant task to evaluate cognitive bias
- **Transition goals/obstacles**: Field test
- **New ideas and whitepapers**: TBD
- **Sponsor relationship, new/additional sponsors**: TBD

Thank you!

David Martinez

dmartinez@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Human Performance: Aptitude

Focus Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Human Performance: Aptitude and Assessment

Susan G. Campbell, Assistant Research Scientist

scampbell@arlis.umd.edu

Objectives: Aptitude and Assessment

- Leverage modern cognitive assessments of skill and aptitude to improve personnel selection and training across the IC, USG, international partners, and commercial partners

Relationship to ARLIS's story

- Aptitude research at ARLIS predates ARLIS, and was a core part of the language mission of the original UARC at UMD
- Problem at that time was finding the right people to do the hardest language work – the stuff you can't automate
- When Cyber became a focus of the IC, the primary sponsor asked the UARC to rapidly pivot to assessing "cyber"
- ARLIS has continued to do this work because it fits within several ARLIS core competencies and spans program areas
- Now also assessing aptitude and proficiency in programming skills for the USAF, building on work in language and cyber

Relationship to ARLIS's goals

- Getting the right people into cognitively complex jobs, especially in work roles related to emerging technologies, will increase capability to perform in advanced missions
- Assessment is also key across a wide variety of other ARLIS program areas: AAA, Human Performance Augmentation, Collective Intelligence, Insider Risk, and any area that involves training or selection
- As researchers, we are uniquely positioned to apply innovative new assessments, and as trusted agents we can evaluate outside assessments across a wide range of applications

Big Wins (so far)

- Cyber Aptitude and Talent Assessment (CATA): UMD Information Systems Invention of the Year in 2021
- High-Level Language Aptitude Battery (Hi-LAB): Finalist for UMD Invention of the Year in 2015
- Clients have included: USAF, USN, USA, USSOCOM, NSA, FSI, DLI, NATO, commercial partners, and foreign government partners (through USG)

Current projects

- CLAB/CLPT: Computer Language Aptitude Battery and Computer Language Proficiency Test
- CATA: Cyber Aptitude and Talent Assessment
- Hi-LAB: High-Level Language Aptitude Battery

Next Steps and Future Capabilities

- New project: CLAB Year 2 starting soon!
- Obstacle: Prospective clients frequently want to purchase a test without any research to fit it to their specific needs
  - Need to make argument that assessing outcomes well and repeatably is necessary for assessing aptitude
- Work on AAA, human performance augmentation will inform new variables to assess and new ways to assess them
  - Continuous assessment from data streams
  - Assessment of core computational thinking skills
- Talking with CYBERCOM, USAF, others in addition to current clients

Thank you!

Susan G. Campbell

scampbell@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

United States Air Force Computer Language Aptitude Battery (CLAB) + Computer Language Proficiency Test (CLPT)

Michael Bunting, Research Scientist, mbunting@arlis.umd.edu

Nick Pandža, Senior Faculty Research Specialist; npandza@arlis.umd.edu

CLAB/CLPT

- Sponsor: United States Air Force
- Program Manager/Client: Roxane Porter; Language, Regional Expertise, and Culture (LREC) Program Office
- Period of Performance: USG FY20, Sep 2019–Sep 2020; New CLAB award: Apr 2021–Apr 2022
- TRL of the work: CLAB: 2 to 5; CLPT 1 to 2
- Total Budget: FY20: $900k / FY21: 650k
- Funding type: 6.2 Applied Research

CLAB/CLPT

ARLIS Team Members

- PI: Dr. Mike Bunting, ARLIS
- Co-PI: Mr. Nick Pandža, ARLIS
- Dr. Noah Silbert, ARLIS
- Dr. Susan Campbell, ARLIS/iSchool
- Dr. Breana Carter, ARLIS
- Ms. Bernadette Jerome, ARLIS
- Ms. Alison Tseng, ARLIS
- Ms. Meredith Hughes, ARLIS
- Mr. Jarrett Lee, ARLIS

UMD iSchool

- Dr. Yla Tausczisk
- Dr. Phil Piety
- Undergraduate Students

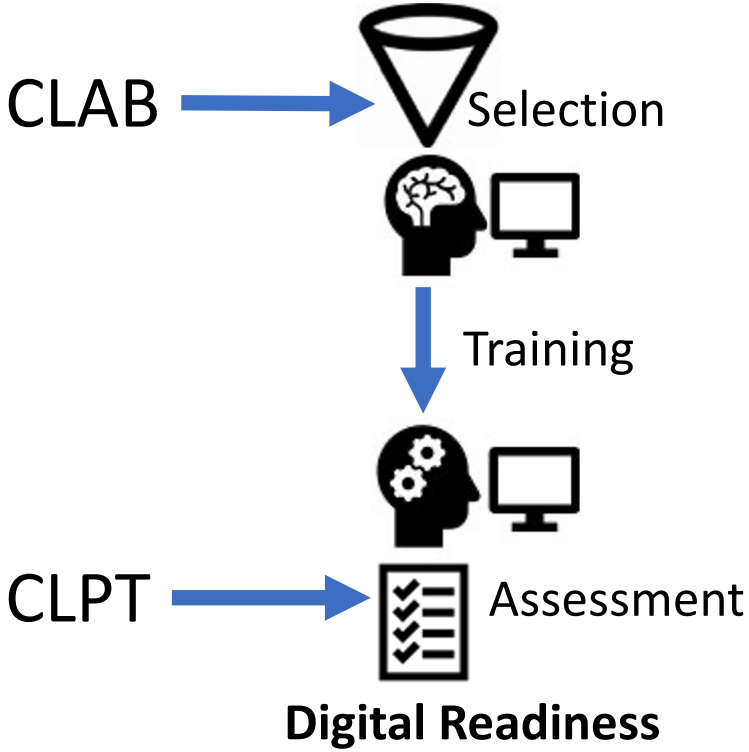
UMD College of Education, Dept of Measurement, Statistics & Evaluation

- Dr. Hong Jiao
- Dr. Robert Lissitz
- Graduate Students

Project Description

Goals

1. Build and validate first-ever USAF aptitude and proficiency assessments for digital talent (software development, data science)
2. Inform USAF talent management approach on training, assignments, and career pathways



Project Description

Current Approach

- Industry: Involved interviews that do not scale
- DoD: ASVAB Cyber Test, manual interview, and/or self-report
- A standardized proficiency scale for digital skills does not exist (cf. Interagency Language Roundtable scores for foreign languages)

Expected Outcome

- Web-delivered assessments that scale easily
- Aptitude test that doesn't require knowledge of digital skills
- Digital skills proficiency framework like the ILR for language skills
- Modular design for distinct and overlapping skillsets (software dev./data science)

Project Description

Measures of Success

- Iterated evidence of reliability and validity
- Ongoing USAF collaboration to ensure the assessments meet their needs

Expected Impact

- CLAB and CLPT will be integral to the USAF's plans for finding, training, and assessing digital talent
- These airmen could go on to support USAF Cyber, conduct Information Operations, or defend systems against insider threats
- Enable expansions of the technical capability of airmen for increased levels of on-the-job automation, regardless of whether their occupation is categorized as computer science-related

CLAB/CLPT Overview

- ARLIS is building:
  - Computer Language Aptitude Battery (CLAB)
  - Computer Language Proficiency Test (CLPT)
- USAF will use these instruments to identify and assess digital talent (software/web devs, data scientists)
  - Potentially use for a Digital Readiness Database
- Could be of interest to all Services, as these types of skills are in high demand and short supply
  - Space Force and Navy have expressed interest

Relationship to ARLIS's goals/story

- Helps identify and assess high demand/short supply programming skills in the DoD
- CLAB leverages existing ARLIS expertise in both aptitude for language learning (Hi-LAB) and aptitude for cybersecurity (CATA)
- CLPT leverages ARLIS's status as a UARC, bringing together top researchers in relevant domains from campus

Big Wins

- Began multiple CLAB validation efforts
  - Content validation with SME interviews
  - In-progress: Contrastive group analysis with USG population
  - Initial assessment for longitudinal validation with USAFA (~1,000 ppl)
- Successfully deployed CLAB v0.1 at scale to incoming USAFA class
- CLAB paper well-received at the Air University LREC Symposium
- CLPT proficiency and testing framework developed for core programming and data science
  - Some initial test items constructed

Project Status

Key Deliverables	Status
(CLAB) 100 Prototype vouchers	Delivered/Accepted
(CLAB) Theoretical Framework	Delivered/Accepted
(CLAB) Longitudinal Validation Plan	Delivered/Accepted
(CLAB/CLPT) Cognitive Task Analysis Content Validation	Delivered/Accepted
(CLPT) Report of USAF Software Engineering Needs	Delivered/Accepted
(CLPT) Test Format	Delivered/Accepted
(CLPT) Scoring Levels & Outcomes	Delivered/Accepted
(CLPT) Proposed Test Content	Delivered/Accepted

Project Status

Project Risk Assessment

- What are the technical risks? Management risks?
  - USAFA and AFCLC are not on the same timeline/contract
- What are the impacts/mitigations?
  - Shift to validation with campus data collection if USG population cannot be found
- What adaptations to your work plan were made due to the COVID-19 pandemic, if any? Were specific actions taken to mitigate impact?
  - Travel canceled; moved to remote interviews and testing
  - May resume in-person interviews/proctoring should COVID-19 restrictions allow

Next Steps and Future Capabilities

- Activities and milestones ahead
  - Additional CLAB funding arrived
  - Next PoP goal to arrive at CLAB v1.0
- Transition goals/obstacles
  - Need additional CLPT funding to create first prototype
- Sponsor relationship, new/additional sponsors
  - Maintaining collaborations (e.g., USAFA, AFCLC, Kessel Run)

Thank you!

Nick Pandža

npandza@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Cyber Aptitude and Talent Assessment (CATA) for SOCOM

Susan G. Campbell, Assistant Research Scientist

scampbell@arlis.umd.edu

CATA for SOCOM

- Sponsor: USSOCOM
- Program Manager/Client: Joint Cyber Operations Group, Ricky Orange, PEO EIS Technology Applications Office
- Period of Performance: 2020-09-01 – 2021-08-31
- Total Budget (+ Expenditures to Date): $109,439 ($65,408)
- Team Members:
  - Dr. Susan G. Campbell, Dr. Breana Carter-Browne, Meredith Hughes, Bernadette Jerome, Alison Tseng, Jarrett Lee

Project Description

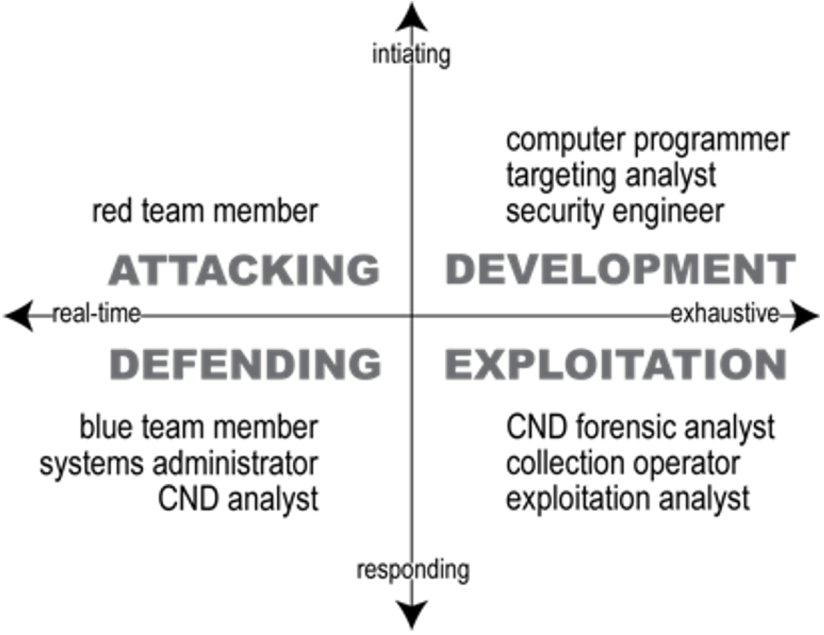
Improving capabilities in the human domain by selecting the right humans for the (cyber) job

Goal: *Enable Joint Cyber Operations Group (JCOG) to select the best candidates for specific roles in their organization*

Expected Impact: *Improving JCOG's effectiveness will improve deployed US cyber capabilities, and extending the use of new selection measures to other organizations will improve US cyber capabilities overall*

Success measures: *Improved person-job fit, improved organizational effectiveness*

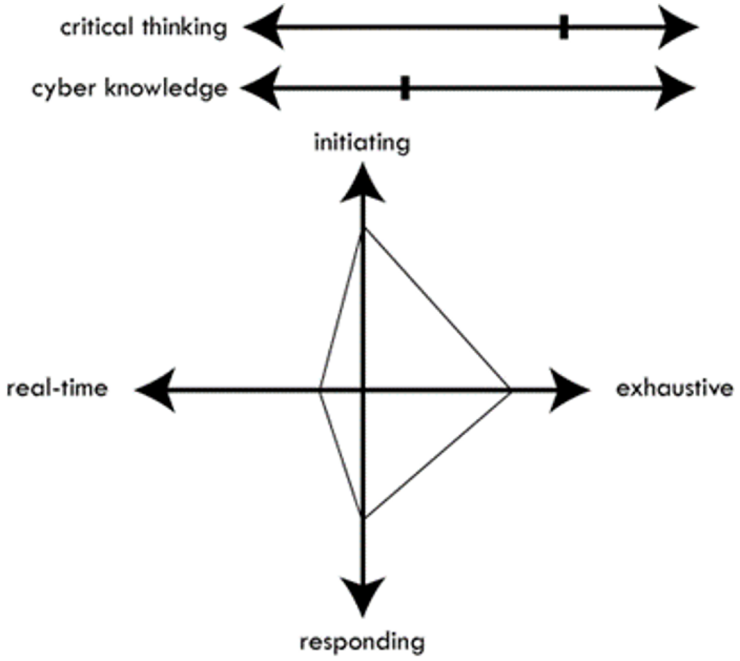
CATA Framework



- Different jobs have different cognitive demands
- Initiating vs. responding axis
- Real-time vs. exhaustive axis
- Initial set of tests developed for each cognitive skill
- Also includes tests of critical thinking aptitude

CATA Scoring concept

- Critical thinking aptitude may be more important for jobs where training is provided
- A person may score well on all, some, or none of the scales
- Tests are behavioral where possible
- Designed to be administered with a cyber knowledge assessment



CATA-SOCOM Overview

- JCOG candidates will take the CATA as part of an accessions, selection, and training (ATS) event
- The ATS cadre will match candidates' CATA profiles to the demands of a particular job in order to determine which person is the best choice for a particular role
- Or the ATS cadre will match the demands of a set of jobs to a particular CATA profile in order to determine which role is the best choice for a particular candidate

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Testing recruits at accessions events	Oct-20, Mar-21	Done
Testing recruits at accessions events	Jun-21, Aug-21	On time
Final report	Aug-21	On time

- **Big Wins (so far)**: CATA is UMD Invention of the Year, JCOG came back for a second year despite contracting hurdles, CATA now delivered on AWS – available everywhere
- **Transition goals/obstacles**: Client wants to transition more administration/scoring to the cadre
- **New ideas and whitepapers**: Looking at measures of team orientation, personality

Thank you!

Susan G. Campbell

scampbell@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Hi-LAB: High-Level Language Aptitude Battery

Ewa Golonka, PI
Associate Research Scientist
egolonka@arlis.umd.edu

Meredith Hughes, Co-PI
Principal Faculty Specialist
mhughes@arlis.umd.edu

Hebrew Hi-LAB: Hi-LAB for Tailored Language Instruction & Improved Personnel Selection

- Sponsor: Army Research LAB (COTR Mitchell Wathen)
- Program Manager/Client: CTTSO (PM Steward Remaly)
- Period of Performance: 09/26/2019–03/14/2021
- Total Budget: $363,606 (Expenditures to Date $360,740)
- TRL of the work: 2 to 7
- Team Members: Golonka (PI), Hughes (Co-PI), Lee, Martinez, Silbert, Tseng, Gardner

Project Description

Long-standing, ever-growing need in the DoD for foreign language skills

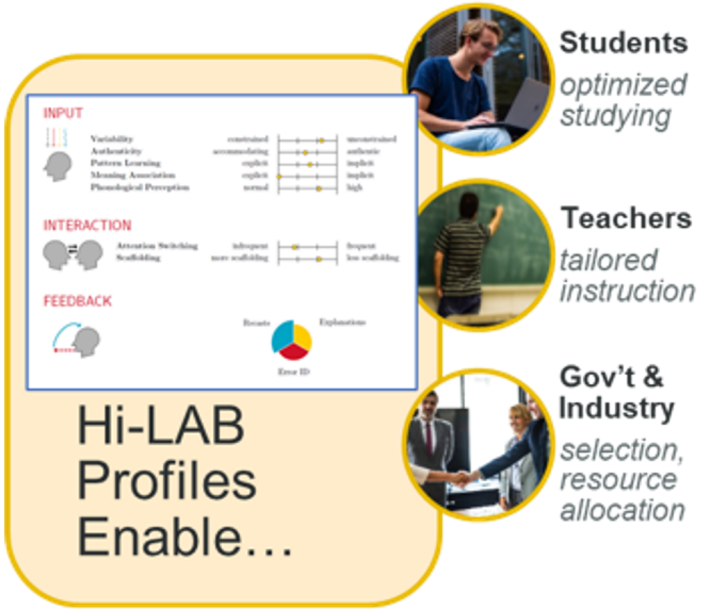
Goal: Better language training outcomes

Select trainees with highest potential
+ Tailor training by aptitude
= More advanced proficiency levels, faster learning for all

Expected impact: Skilled personnel, more effective in performing job tasks

Success measures: Validated Hebrew Hi-LAB test battery, scalable methodology, satisfied client

Hebrew Hi-LAB



Project objectives:

- Adaptation of Hi-LAB for Hebrew speakers
- Usability, psychometric, and preliminary validation studies
- Power analysis of historical data
- Technology transfer

Project status:

- Work completed: functioning software; development and validation reports; tech transfer

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Hi-LAB Test & Training Suite: Software/Virtual Machine	Completed	On schedule
Development Test & Eval/Customer Acceptance Test & Training	Completed	On schedule
Pilot Test Reports	Completed	On schedule

- **Big Wins**: Product used in high-stakes environment; improved Aptitude Profiles to benefit US test-takers; secured service contract; client open to future collaboration; publications
- **Transition goals/obstacles**: Technology successfully transferred
- **New ideas and whitepapers**: Aptitude-by-treatment teacher-training and experimental studies
- **Sponsor relationship, new/additional sponsors**: Continue relationship with CTTSO, ARL, international partner

Thank you!

Ewa Golonka
egolonka@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

ARLIS Program Reviews, v3.0 Series 2021

Day 2 – Tuesday 4 May 2021

Wednesday 5 May	
0900 – 0915	Overview of the Day
0915 – 0945	**Computational Infrastructure**
0945 – 1035	**Data Curation and Resource Building**
1035 – 1045	*Break*
1045 – 1125	**Testbeds and Subject Matter Expertise**
1125 – 1210	**Managing & Mitigating Insider Risk**
1210 – 1300	*Lunch break*
1300 – 1410	**Acquisition and Industrial Security**
1410 – 1445	**Augmented Collective Intelligence**
1445 – 1500	*Break*
1500 – 1530	**FY22 Internal Research & Development Projects**
1530 – 1540	**The Intelligence & Security University Research Enterprise Consortium**
1540 – 1610	**Training and Workforce Programs**
1610 – 1630	Wrap-Up

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY
UNIVERSITY OF MARYLAND

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

ARLIS Computational Infrastructure

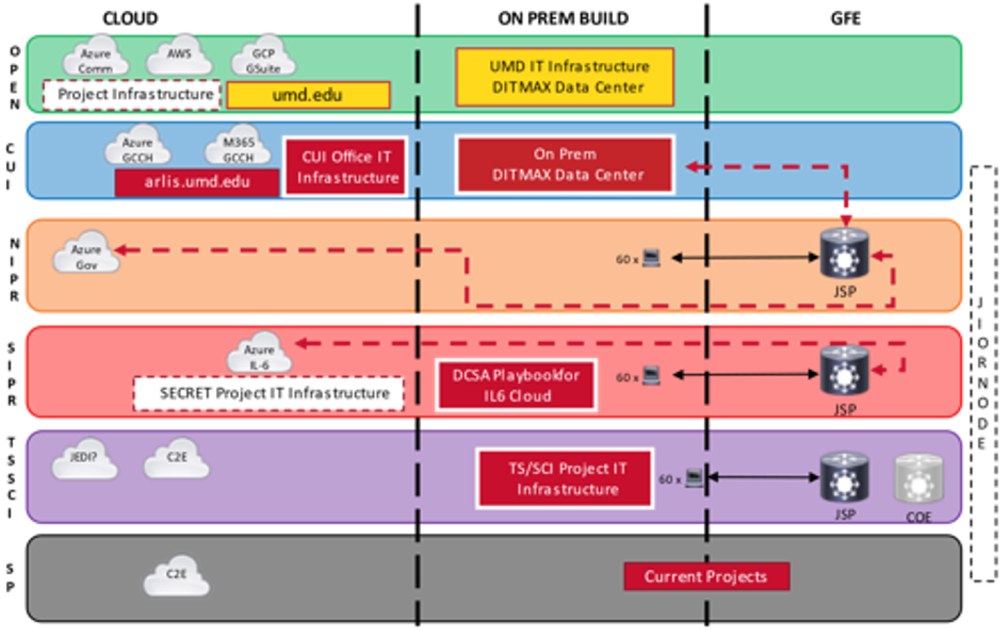
Joe Kelly, Interim Director of Computational Infrastructure

jkelly@arlis.umd.edu

Mission Area Objectives: Computational Infrastructure and Technology

- ARLIS as co-location R&D facility for DoD & IC
- Computational and IT infrastructure foundation for Mission Areas
- Multi-tenant, Multi-level Security, Federated Governance
- Facilitate integration of US government capabilities and assets
- Repository of data and code
- Flexible environment for diverse research

Mission Area Objectives: Computational Infrastructure and Technology Overview



- Multitenant
- Multilevel security
- Scalable
- Active and archive storage at scale
- Large scale data transfer
- Cross-domain solutions
- Track usage and assign costs

Relationship to ARLIS's goals/story

- Foundation for ALL Mission Areas
- Only UARC building extensible CUI cloud environment
- Apply CUI lessons to classified cloud environments
- Trusted partner for US Government evaluation of cloud
- Expand to HPC via INSURE Consortium (including classified)
- Expand to quantum computing and other novel research areas

Big Wins (so far)

- Microsoft Partnership on CUI and Azure SECRET
- Validation of Need from DARPA, IARPA, NGA, CENTCOM, SOCOM, Army PEO STRI, Navy NIWC Atlantic, Air Force SAF/CDM
- OUSD(I&S) Brokering Introductions to other CSPs

Team Members

- PI: John Romano
- ARLIS Team Members: Joe Kelly, Joe Jaucian, Gerhard Bartsch, Jarrett Lee, Gene Gualtieiri, Brian Shoemaker, Sonia Morgan, Enrico De LaPaz, Saquan Pray, Gabrielle Bonny
- Other Team Members: Kevin Hillibrand (UMD DIT MAX), William Burns (consultant - past CASL staff), Planet Technologies (migration contractor), Microsoft, with others to be added

Computational Infrastructure Task

- Sponsor: OUSD(I&S) [base funding] ARLIS [ongoing]
- Program Manager/Client: Amanda McGlone
- Period of Performance: 5/18/20-10/31/21 [assumes NCE approval]
- Total Budget (+ Expenditures to Date): $3.95M
- TRL of the work: 6/7
- Team Members:
  - PI: John Romano
  - Joe Kelly, Joe Jaucian, Sonia Morgan, Brian Shoemaker, DIT MAX
  - Planet (migration support); Microsoft (vendor)

Computational Infrastructure Description

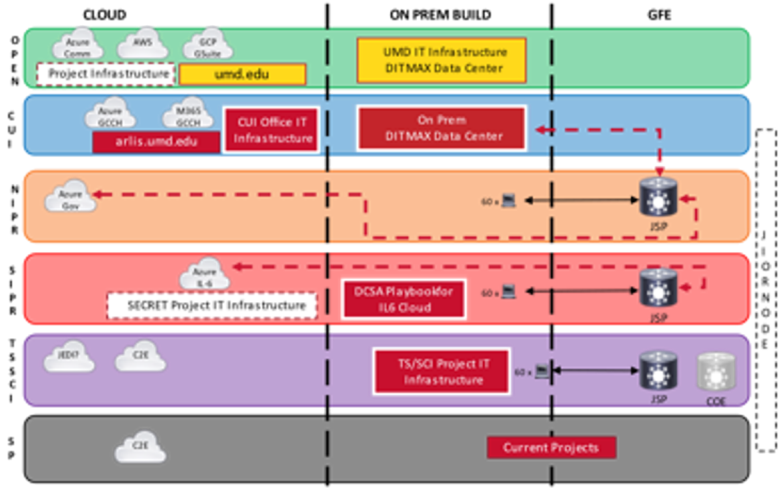
Computational Infrastructure: OUSD(I&S) funding creation of initial CUI and TS/SCI environments for ARLIS and establishing mechanisms by which ARLIS can operate IT systems from open Internet to special program level.

Goal: Create basic infrastructure and work through approval processes for provisioning research IT infrastructure at CUI, SIPR, and TS/SCI levels.

Expected Impact: Demonstrate feasibility of creating multi-tenant multi-sponsor IT infrastructures across all levels of classification

Success measures: Signed ATOs for classified enclave; NIST 800-171 controls established for CUI

Computational Infrastructure Overview



Tasks:

- CUI Environment – Both Core Office & Research Elements
- TS/SCI Enclave - Standalone
- DCSA Draft Playbook for Azure IL-6 (SIPR Cloud for CDCs)*

Deliverables:

- CUI Compliant Enterprise IT System for ARLIS
- TS/SCI Enclave ready for ATO
- Draft Playbook for DCSA to guide Azure IL-6 Approvals for Contractors

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
CUI Environment (w/Microsoft)	31 Oct 2021	
TS/SCI Environment	31 Oct 2021	
New Task – DCSA Playbook	30 Sep 2021	

- **Issues:**
  - CUI research environments and CUI Office 365 should be ready by August
  - CUI processes and controls will continue to evolve through 31 October 2021
  - TS/SCI environment will need authorization
  - DCSA Playbook is dependent upon cooperation from candidate cleared defense contractors

Thank you!

Joe Kelly
jkelly@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Data Curation & Resource Building

Mission Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Data Curation and Resource Building

Michelle Morrison, Associate Research Scientist
mmorrison@arlis.umd.edu

Program Area Objectives: Data Curation and Resource Building

- Develop and maintain a reputation for provision of **gold standard data** that underpins technological innovation
- Serve as the **IC's trusted partner** for any challenge that involves data provisioning and annotation
- **Integrate human and automated processes** in the curation of purpose-built datasets that serve a wide range of analytic purposes

Relationship to ARLIS' goals/story

- The IC has **critical needs** for data collection, data processing in the human domain
- ARLIS is uniquely positioned to provide **language, technology, and program expertise** to help solve USG/IC problems
- Technologies such as information retrieval, information extraction, event detection, named entity recognition, automatic speech recognition, optical character recognition, etc. are only successful if they are trained on **high quality, gold standard annotated data**
- The UARC has a long history (10+ years) serving on IARPA (and more recently, DARPA) T&E teams for various programs, esp. HLT/NLP-related
- Synergy with other mission areas (e.g., Cognitive Security) that rely on large datasets and/or naturalistic data

ARLIS' Unique Capabilities

- Other organizations are often reluctant to work on projects that involve data that is **1) multilingual**; 2) in a **low-resourced language**; 3) written in a **non-Roman script**; 4) written with **variable spelling and grammatical conventions**
  - ARLIS has strengths and documented history of success in precisely these areas
- ARLIS has a demonstrated ability to **quickly stand up annotation pipelines in multiple languages with complex annotation schemas**
- Strategies developed for previous data curation projects are easily extensible to other open-source datasets and data types
- **Multiple strategies**, dependent on project needs:
  - Local, in-person collaboration
  - Virtual collaboration
  - Collaboration with visiting foreign scholars

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Support to IARPA MATERIAL

Michelle Morrison, Associate Research Scientist

mmorrison@arlis.umd.edu

MATERIAL

- **Sponsor**: IARPA
- **Program Manager/Client**: Carl Rubino
- **Period of Performance**: 2017-2020
  - Final POP: September 5, 2019-October 4, 2020 (project has concluded)
- **TRL of the work**: 3/4
- **Total Budget** (+ Expenditures to Date):
  - $728,464 in final POP
  - $2,781,941 over the course of the project

Team Members

- **PI**: Michelle Morrison
- **co-PI**: Aric Bills
- **FRS**: Sara McConnell
- **PC**: Chris Gardner
- **Admin** Support: Caitlin Eaves (LSC)
- **Undergraduate RA**: Sarah Marvi
- **Six visiting scholars from overseas** (Georgian and Kazakh)
- **Three C-1s** (Farsi)

Project Description

MATERIAL goal: Revolutionize **multilingual triage** by enabling rapid development of language-independent methods to build systems capable of fulfilling domain-specific **cross-language information retrieval** tasks over both text and speech data, with English query in and English summary out.

ARLIS' role is to facilitate program success by:

- Developing and testing program parameters;
- Advising on language selection;
- Producing program evaluation data (queries);
- Providing expert linguistic and program knowledge to support T&E

Project Description

How is it done today (+ by whom?), and what are the limits?

- QA/QC: mostly automated methods, with little human review
- (CL)IR query development: Programs are designed around very large amounts of (mostly text) data, queries are long, up to paragraph length, post-hoc human evaluation of subset of documents returned as potentially relevant; resulting in large corpus (hence focus on well-resourced languages) with very small numbers of queries

By whom?

- Query development: NIST (others?)
- Data collection/annotation: Appen, LDC (we have collaborated with both)

Project Description

Expected Outcome:

Success of the program will allow analysts and others to use English language queries to search non-English sources, dramatically pushing ahead technologies in Cross Language Information Retrieval.

Success measures:

- Direct measures of ARLIS success: produce contractual number of queries (query targets exceeded)
- Indirect measures of ARLIS success:
  - Queries allow for differentiation of performer teams
  - Success of performer teams

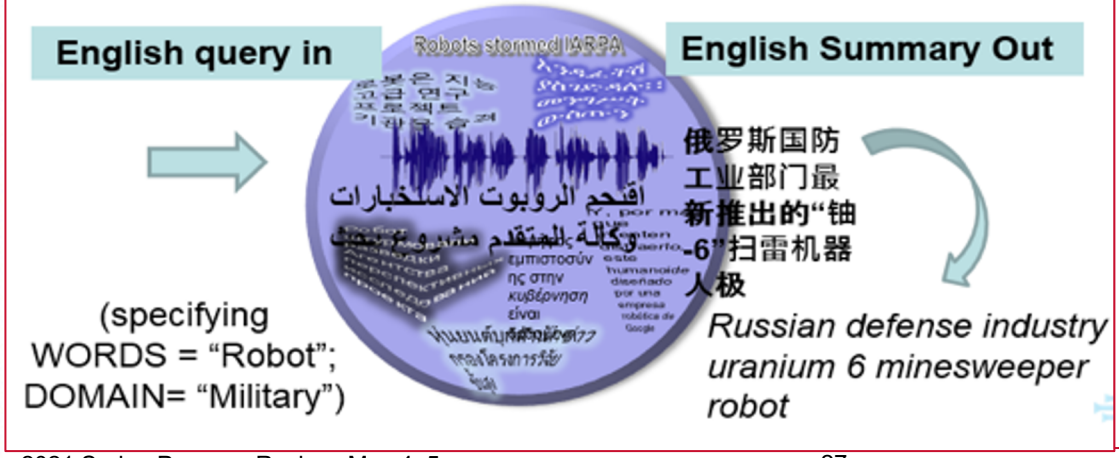
Life Cycle of a Query

			2B Lithuanian	2C Pashto	2S Bulgarian	3B Georgian	3C Kazakh	3S Farsi
Lexical	868	972	669	416	691	887	781	858
Conceptual	417	481	255	260	299	366	384	410
Morphological	136	137	185	84	135	--	--	--

MATERIAL

MATERIAL Goal: Revolutionize multilingual triage by enabling rapid development of language-independent methods of cross-language information retrieval over both text and speech, via English-in-English-out end-to-end system.

ARLIS Role: Apply language and program expertise to develop and implement successful program, including production of ground-truth data for program evaluation in multiple languages.



Project Status: MATERIAL program is in its final year; ARLIS' role has concluded.

Relationship to ARLIS's goals/story

- We supported a program that will revolutionize how analysts do their jobs and how foreign language data is both made accessible and triaged.
- The UARC has a **10-year relationship** with IARPA serving on T&E teams for various programs, esp. HLT/NLP related.
- **Critical IC needs** for data collection, data processing, and data analytics, mostly in foreign, low-resource languages.
- ARLIS/UMD is uniquely placed to provide language, technology, and program expertise to help solve USG/IC challenges.

Big Wins (so far)

- Successful **on-time completion** of the project; **exceeded query targets** in all three languages
- Developed a process to bring **international scholars** to College Park to work on ARLIS projects
  - Novel approach allowed us to take advantage of cutting-edge expertise on low-resourced languages
- The development of **novel query types and methodology** are pushing development of IR/CLIR in new directions, in new languages
- Developed **virtual annotation workflow** which can extended to other projects
- Success on MATERIAL led to funding for BETTER T&E
- T&E publication: Zavorin, Ilya, Aric Bills, Cassian Corey, Michelle Morrison, Audrey Tong, and Richard Tong. *Corpora for Cross-Language Information Retrieval in Six Less-Resourced Languages*. LREC 2020.
- 94 peer-reviewed publications from the program as a whole, to date.

Project Status

Deliverable	Contractual Target	Queries delivered	Status
3B Lexical Queries	715	887 (124%)	Delivered
3B Conceptual Queries	310	366 (118%)	Delivered
3C Lexical Queries	715	781 (109%)	Delivered
3C Conceptual Queries	310	384 (124%)	Delivered
3S Lexical Queries	715	858 (120%)	Delivered
3S Conceptual Queries	310	410 (132%)	Delivered
3S Post-Hoc Queries	added in NCE	217	Delivered

Thank you!

Michelle Morrison
mmorrison@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

KAIROS (Knowledge-directed Artificial Intelligence Reasoning Over Schemas)

Aric Bills, Principal Faculty Research Specialist

abills@arlis.umd.edu

Support for DARPA KAIROS

- Sponsor: DARPA (sub to University of Pennsylvania Linguistic Data Consortium)
- Program Manager/Client: Eduard Hovy (DARPA); Stephanie Strassel (LDC)
- Period of Performance:
  - Phase 1: Sept. 9, 2019 – Mar. 9, 2021
  - Project extends to Sept. 9, 2023
- TRL of the work: 3
- Total Budget (+ Expenditures to Date): $423,205 ($323,679 spent to date)
- Team Members (co-PIs, sub awardees):
  - Aric Bills (PI), Michelle Morrison (co-PI),
    Jarrett Lee, Tess Wood, Brenda Clark, Sandra Panolis, Zachary Deaton
  - Emeritus: Tom Conners, Nikki Adams

Project Description

Goal:

Overall program: Develop a schema-based AI system that can identify complex events and bring them to the attention of users.

ARLIS: Help LDC build libraries of schemas, gather media exemplars, and provide non-obvious ways of QC for annotation of target event types in media.

SWOT: Most annotation QC is built on a presumption that there should be agreement between annotators, but event detection annotation frequently has poor agreement.
QC in this situation regularly involves outlier detection, but not much beyond that.

We have been developing strategies to find annotation that is truly problematic, not simply different. Jarrett developed a GUI for annotation review that allows us to visualize complex relationships between elements of annotation and direct the reviewer's attention to potential issues.

Project Description

Expected Outcome: Analyst systems will be able to learn complex event schemas from big data and apply these to multimodal, multilingual information to discover and extract complex events.

Success measures:

- ARLIS regularly finds problematic annotation that LDC did not find through its simpler checks
- Performer teams successfully use QC'ed data to learn event schemas, discover/extract complex events

KAIROS Overview

KAIROS envisions a future in which:

- Analysts will be able to define “event complexes” (directed graph representations of events that occur together in service of one or more goals)
- Systems will leverage ontological knowledge and prior experience to recognize instances of event complexes in different media and languages, with little to no new annotated training data
- Ultimately, systems will predict future events based on recognition of elements of event complexes

Relationship to ARLIS's goals/story

- Analysts are good at identifying complex patterns that signal threats to national security; KAIROS aims to give them better ways to tell a computer system what to look for
- Synergies with IARPA BETTER
  - Different ways of approaching the nature of events, participants, etc.
  - Opportunities to analyze annotator agreement given complex annotation schemes
- Furthers ARLIS's role as a trusted T&E partner

Big Wins (so far)

- Worked with LDC to create, refine, group and finalize 100 complex events
- Jarrett's QC tool makes it easy to analyze multi-faceted questions about complex annotation across multiple documents

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Development/review of complex events	Delivered	On sched
Review of scouting corpus documents	Delivered	On sched
Review of scouting corpus annotations	Delivered	On sched
Review of schema learning corpus annotations	Not delivered	Issue

Project Risk Assessment

- Funds were exhausted in January; awaiting next funding increment (as of 4/23)
- Stopped work 1/29/21; expect funding within next two weeks
- May need to recruit new help due to gap in funding
- Few adaptations needed to adapt to COVID-19
  - Moved meetings to Zoom
  - Able to hire very talented people who were underemployed due to pandemic

Next Steps and Future Capabilities

- Program is transitioning from a bespoke ontology to a larger, general-purpose ontology (DWD)
- More complex representation of events
- More finely-specified temporal relations between events

Thank you!

Aric Bills

abills@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Support to IARPA BETTER

Michelle Morrison, Associate Research Scientist

mmorrison@arlis.umd.edu

Support to IARPA BETTER

- **Sponsor**: IARPA
- **Program Manager/Client**: Carl Rubino
- **Period of Performance**:
  - Phase 1: July 13,2020 – April 1, 2021 (complete)
  - Phase 2: April 1, 2021 – September 30, 2021
- **TRL of the work**: 3/4
- **Total Budget** (+ Expenditures to Date):
  - Phase 1: $604,000 (expended)
  - Phase 2: $1,713,456
- **Team Member**:
  - ARLIS/UMD team: Michelle Morrison, Valerie Novak, Aric Bills, Victor Frank, James Hull, Tess Wood, Christopher Gardner
  - Annotators: Arabic (x3); Farsi (x3); Phase 3 Language (x7)

Project Description

Program Goal: Develop methods for extracting increasingly fine-grained semantic information, with a focus of events in the form of who-did-what-to-whom-when-where, across multiple languages and problem domains

- Train on English; test on target language(s)

ARLIS role: Provide high quality annotated data for events (who did what to whom?) in a complex annotation schema

- Four languages (possibly six); three different scripts
- Three levels of annotation (Abstract, Basic, Granular)

Project Description

SWOT: How is it done today (+ by whom?), and what are the limits?

- Annotation projects often cut corners in annotation as a cost-saving measure (e.g., relying on Amazon Turkers), resulting in poor quality annotation with high variability
- Annotation of non-English materials often done on machine translated output
- High quality annotation often becomes cost prohibitive to produce – need for workflow that appropriately balances quality and cost
- Some data providers reluctant to work on lower-resourced languages and/or languages in non-Roman scripts

Project Description

Expected Outcome:

- Enable the USG and performers to develop complex information extraction and information retrieval systems using accurate and consistent data

Measures of success:

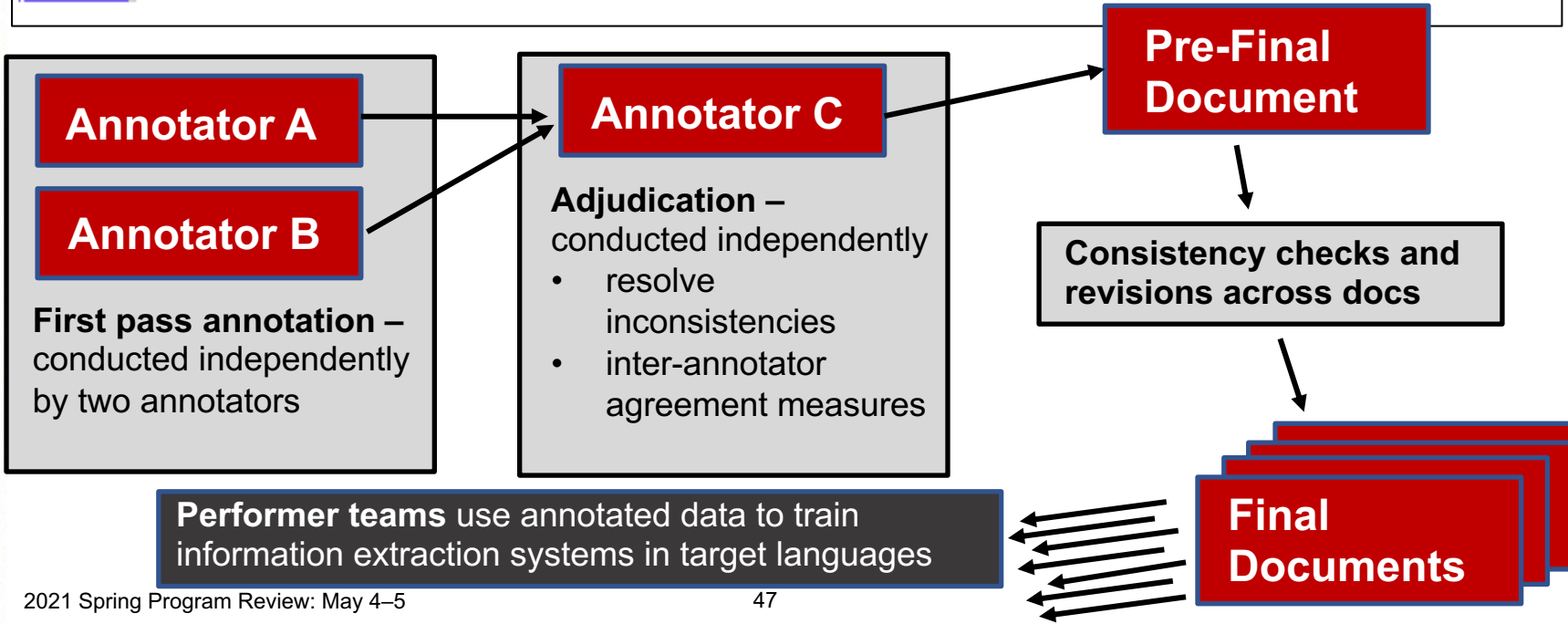
- Inter-annotator agreement;
- Quantity of annotated data provided across number of languages
- Feedback and results from client and performer teams

Expected Impact:

- Analysts will be able to work through large amounts of data in multiple languages, better understanding relationships between events and entities (who's doing what to whom?)

BETTER Workflow

Egypt is fighting an insurgency by militants affiliated with ISIS in the Sinai Peninsula, where hundreds of soldiers and police have been killed since 2013 when the military ousted Islamist president Mohamed Mursi after mass protests.



Relationship to ARLIS's goals/story

- Analysts are overwhelmed with data – need for better technologies to enable them to swiftly sort through data in multiple languages and draw relationships between events and entities
- *"Garbage in, garbage out"* – new technologies are only as good as data upon which they are trained; good, high quality annotated datasets are in high demand
- ARLIS is developing a reputation as a reliable partner on T&E projects

Big Wins (so far)

- Success in Phase I resulted in second period of performance; potential for two additional languages in Phase III
- Positive feedback from Program Manager and Director of IARPA
- COVID as an opportunity to transform workflow
  - Previous annotation projects relied on local annotators
  - Adaptation of annotation process to a fully virtual workflow has enabled us to tap into expertise across the country
- Demonstrated ability to quickly stand-up annotation pipeline in multiple languages with a complex annotation schema

Project Status

	Key Deliverables/ Insights / Activities	Timeline/ status
BETTER POP 1	Arabic: Basic (2,024 events) + Granular (112 templates)	Delivered
	English: Granular (131 templates; 153 files)	Delivered
	Farsi Abstract (15,005 events)	Delivered
	Phase 3 Language Abstract (16,704 events)	Delivered
BETTER POP 2	Phase II English Basic (7/1/21) + Granular (12/1/21)	On track
	Farsi Corpus Development (10/1/21)	On track
	Farsi Basic (11/1/21) + Granular (2/1/22)	On track
	Language 3A Corpus Development (1/1/22)	Not started
	Language 3A Basic (2/1/22) + Granular (8/1/22)	Not started

POP 2 Targets (per language): Corpus Development: 800,000 documents; Basic: 2,000 unique events; Granular: 475 templates

Project Risk Assessment

- Initial work in Phase 1 was delayed due to issues out of our control (no data to annotate; delay in receipt of annotation guidelines); however, we requested an NCE and were able to deliver all annotations within a timeframe that allowed the program to proceed on schedule
- Lessons learned in Phase I are informing work plan/timeline in Phase II
- Complex annotation schema with multiple annotators presents challenges in consistency
  - Frequent meetings; use of collaboration technology
  - Measures of inter-annotator agreement (new in Phase II)
- UMD hiring: Annotators are typically hired as C-1 hourly employees or as contractors; this works well for short-fuse projects, but becomes problematic for projects with longer term hiring needs (but gaps in funding)

Next Steps and Future Capabilities

- Activities and milestones ahead: beginning Phase II
  - Develop Phase II annotation guidelines
  - Annotation of Phase II materials (English and Farsi; Basic and Granular)
  - Planning and preparation for Phase III (+potential new languages for Phase III)
- New ideas and whitepapers
  - Potential collaboration with Accenture: annotation for social unrest
  - Computational Cultural Understanding (T&E for new DARPA project)
- Sponsor relationship, new/additional sponsors
  - Continued positive relationship with IARPA
  - Additional T&E work on other programs

Thank you!

Michelle Morrison
mmorrison@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Trusted Work: Testbeds and Subject Matter Expertise

Program Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

GATR Project MANTRA

Joe Kelly, Professor of Practice

jkelly@arlis.umd.edu

GATR Project MANTRA

- Sponsor: Air Force, SAF/CDM
- Program Manager/Client: Elizabeth Chamberlain
- Period of Performance: 2/1/21-8/2/21
- Total Budget (+ Expenditures to Date): $250K
- TRL of the work: n/a – study only
- Team Members:
  - PI: Joe Kelly
  - Gil Martinez
  - Govini

Project MANTRA Description

Project Mantra is a study on DoD use of publicly/commercially available information (PAI/CAI) where ARLIS will evaluate the scope of PAI/CAI use and make policy recommendations.

Goal: Provide insight on scope of DoD PAI/CAI use and highlight policy issues

Expected Impact: Create framework for DoD to track and manage PAI/CAI use

Success measures: Ability to use DoD data catalogue for PAI/CAI management

Project MANTRA Overview

- MANTRA
  - Augments earlier OSD data call on PAI/CAI with new info;
  - Tests ability to identify PAI/CAI end user from contract data;
  - Bins use cases for PAI/CAI for policy recommendations
- For DoD Chief Data Officer:
  - Determine viability of data catalogues for managing PAI/CAI
- For SAF/CDM:
  - Ensure sound policy guidance on operational use of PAI/CAI

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Phase 1 Report	5 March 2021	Delivered
Research	Ongoing	Delayed
Final Report	30 June 2021	On track

- **Issues:** Hiring delays slowed research; back on track
- **Big Wins (so far)**: Phase 1 report validated limits of data call
- **New ideas**: Policy rubric – rules for PAI/CAI use including OSINT
- **SAF/CDM**: Project MAYA follow on to track PAI/CAI sources and tech

Thank you!

Joe Kelly
jkelly@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

DARPA Food & Agricultural Assurance & Supply Chains Testbed (FAAST)

Polly O'Rourke, Associate Research Scientist

porourke@arlis.umd.edu

DARPA FAAST

- Sponsor: DARPA DSO
- Program Manager/Client: Randy Garrett
- Period of Performance: 4/16/21 – 1/15/22
- Total Budget (+ Expenditures to Date): $2.2M ($0.00)
- TRL of the work: 2

DARPA FAAST

Team Members (co-PIs, subawardees):

- PI Polly O'Rourke
- Team Members:
  - **ARLIS**: Bill Regli, Gene Gualtieri, Michelle Morrison, Brook Hefright.
  - **UMD Center for Global Agricultural Modeling Research**: Inbal Becker-Reshef, Michael Humber, Estefania Puricelli
  - **Renssaeler Polytechnic Institute**: Deborah McGuinness, Jim Hendler
  - **Information Sciences Institute at USC**: Craig Knoblock, Pedro Szekely

Shout out to Joe Kelly, Chris Gardner, Bret Howard, Monique Anderson and Adam Grant

Project Description

Goal:

- Integrate disparate datasets related to food and agricultural supply chains into testbed.
- Provide previously undiscovered insights and predictors of disruptions/vulnerabilities.
- Brazil, Nigeria and Thailand are the countries of focus.

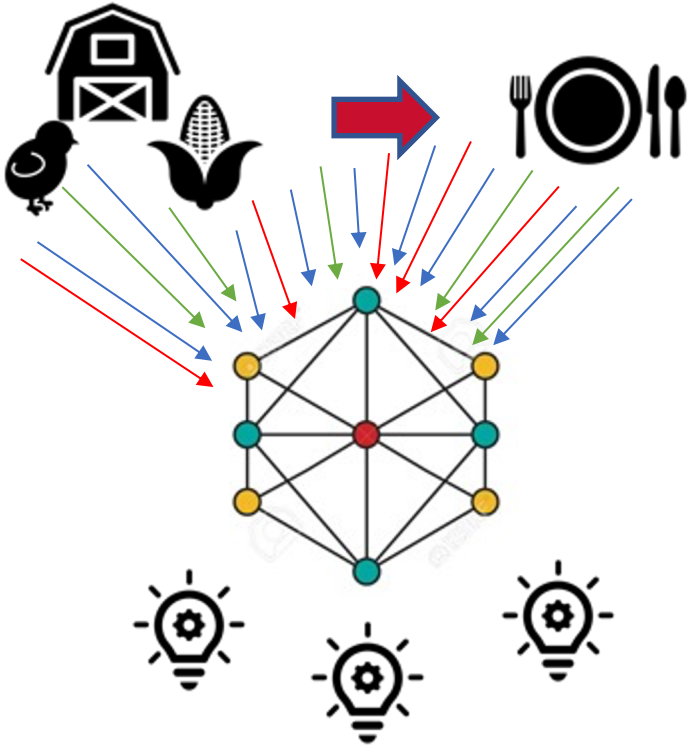
Expected Impact:

- Enhanced actionable intelligence insights relating to food security.

Success measures:

- Successful integration of disparate datasets;
- Interoperability across datasets/types,
- Meaningful anomalies in the associations and predictors related to disruption of food and agricultural supply chains.

DARPA FAAST Overview



Project objectives

- Ingest multiple disparate datasets.
- Develop information architecture that supports interoperability.
- Identify unexpected patterns / predictors relating to food supply chain security.

Project status

- PoP began 4/16
- On time for all milestones and deliverables.

Thank you!

Polly O'Rourke

porourke@arlis.umd.edu

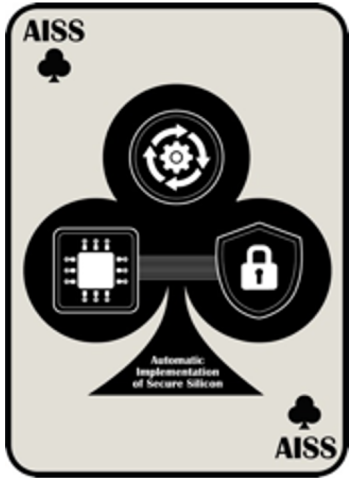
Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

DARPA AISS Program

Automatic Implementation of Secure Silicon



Warren Savage, Principal Investigator, AISS IV&V

tws@umd.edu

AISS Program IV&V Task

- Sponsor: DARPA MTO
- Program Manager/Client: Serge Leef
- Period of Performance: August 2020 – May 2024
- Total Budget (+ Expenditures to Date): $4.96M ($572K spend to date)
- TRL of the work: none (IV&V is focus)
- Team Members (co-PIs, subawardees):
  - Jana Schwartz (UMD ARLIS)
  - Ankur Srivastava (UMD Institute of Systems Research)
  - Ramesh Karri (NYU)
  - Adam Porter (Fraunhofer USA)

Project Description

ARLIS Value Proposition:

Bringing together industry and academic experts for thorough assessment of AISS deliverables

Goal:

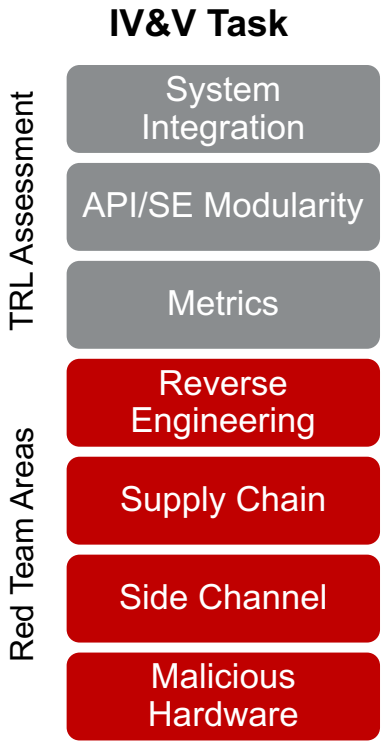
High TRL enabling rapid deployment to industry and DIB

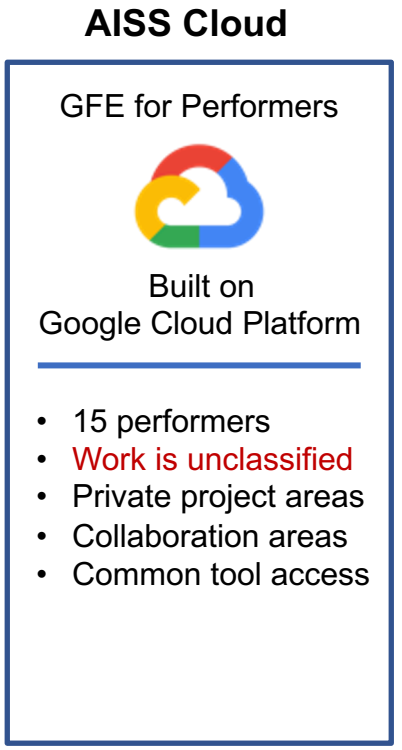
Expected Impact:

Democratization of *design-for-security* in chip design (new capability, adhoc today)

Success measures:

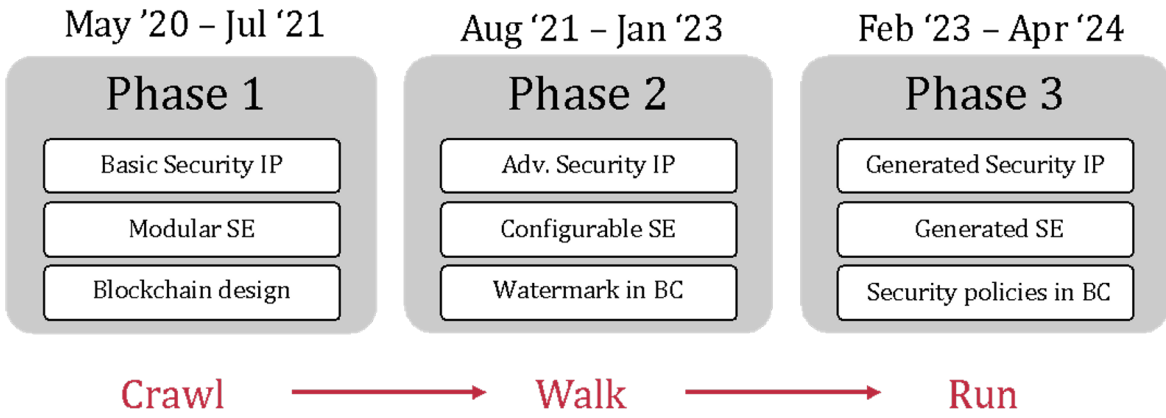
Rapid adoption by the DIB immediately following program. (Note: Proposers are already promising use of AISS as part of RAMP program)



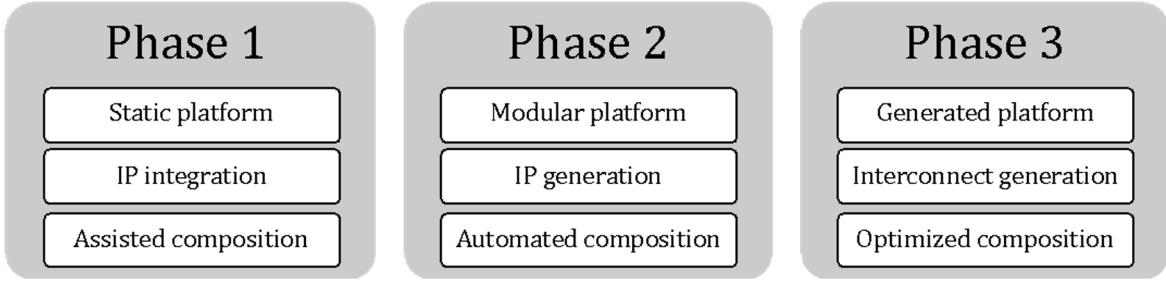


AISS Overview

TA1 – Security Engine
- Security IP blocks
- Security engine
- Blockchain infrastructure



TA2 – Platform
- Core platform
- Infrastructure
- Composition



Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
AISS Cloud	Operating	On sched
IV&V	Continuous	On sched

Big Wins (so far):

- AISS Cloud deployed – custom Cloud a possible blueprint for future interagency collaboration
- Deep technical feedback being delivered to performers for course correction

Transition goals/obstacles:

- Goal is to achieve TRL 6-7 by end of program for rapid deployment into industry

New ideas and whitepapers:

- Novel Trojan attack/defense measures

Sponsor relationship, new/additional sponsors:

- Other similar approaches for “agile IV&V” that is done concurrently with program execution

Thank you!

Warren Savage

tws@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Electronic Warfare Study and Plan

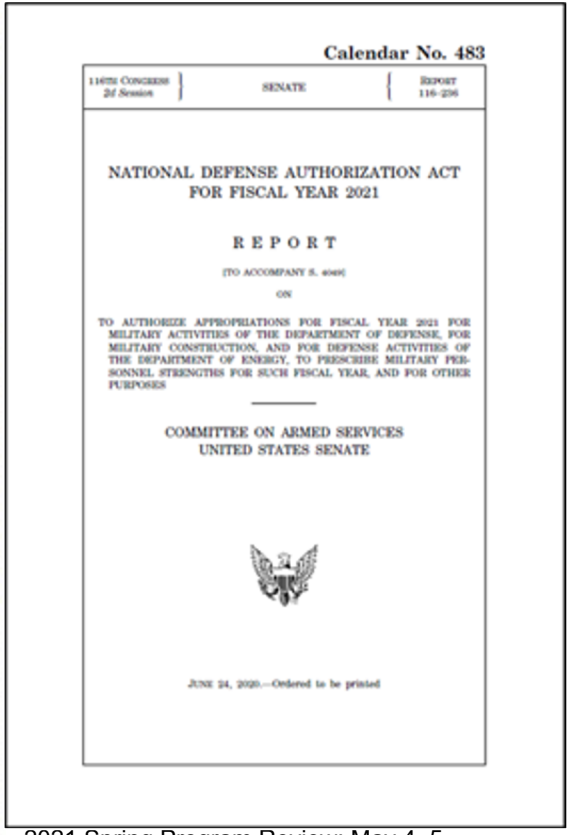
Joe Kelly and Austin Branch, Professors of Practice

jmkelly@umd.edu abranch1@umd.edu

Electronic Warfare Study (Phase One)

- **Sponsor:** Army Threat Systems Management Office (TSMO) and OSD P&R
- **Program Manager/Client:** Army TSMO
- **Period of Performance:**
  - Phase 1 (Oct 2020 – July 2021);
  - Phase 2 & 3 TBD
- **Total Budget:** 400K ($xxx expended)
- **TRL of the work:** N/A
- **Team Members:** Corvus Inc.

Congressional Direction



Calendar No. 483

116TH CONGRESS 2d Session | SENATE | REPORT 116-236

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021

REPORT

[TO ACCOMPANY S. 4049]

ON

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2021 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE, FOR MILITARY CONSTRUCTION, AND FOR DEFENSE ACTIVITIES OF THE DEPARTMENT OF ENERGY, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

JUNE 24, 2020.—Ordered to be printed

As requested by Senate Report 116-236, page 54, Section 4049, Accompanying the National Defense Authorization Act for FY21

The committee recognizes the requirement for the Department of Defense (DOD) to operate across the electromagnetic spectrum and prevail in electronic warfare (EW) in every operational domain. **Development of capabilities needed to control the EW battlespace requires well-developed training ranges that enable the military services and Defense Agencies and Field Activities to rapidly test and field new weapon systems.** Increased demand and spectrum encroachment at current EW training ranges mean that these facilities are inadequate to meet the Department's EW test and training needs over the next several years. **Therefore, the committee directs the Secretary of Defense to provide a plan for the establishment of a Joint Electronic Warfare Training Range that: (1) Offers sufficient space for spectrum isolation; (2) Provides for the ability to protect sensitive technologies from detection by offering access to large, inland space; and (3) Would be specifically dedicated to EW activities to avoid overcrowding. This plan shall be briefed to the congressional defense committees…**

Background:

- The DoD Chief Information Officer (CIO) is funding this study and plan through an above threshold reprogramming action in the Army RDT&E APE 664256976 for the amount of $3M.
- TSMO funded initial 400K for study via purchase order

- The intent is to determine how to improve spectrum operations on training ranges and to examine improvements for EW training.

- Approach will be executed in Three Phases:
    1. Study and Analysis (Funded and in execution)
    2. Concept Development
    3. Plan Development

EW Study Phase One Study

Key Tasks (Phase one- Study):

- Identify the spectrum management and automation capabilities needed in spectrally congested training range operations.
- Identify opportunities to increase operational EW training range infrastructure including threat systems and live, virtual, constructive (LVC) enablers consistent with JOTI..
- Recommend how to Enable EW in all training environments and incorporate EMS as a warfighting maneuver space---pivoting and or building from existing efforts.
- Recommend how to align with national spectrum policies; leverage the opportunities of rapid technological innovation and 5G networks/communications; and mitigate attendant vulnerabilities and threats.
- Identify areas of potential integration into CEMA and Information Dominance efforts

Purpose:

- Develop superior EMS capabilities.
- Evolve to an agile, fully integrated EMS infrastructure.
- Pursue total force EMS readiness.
- Integrate into broader CEMA and Information Dominance efforts

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Phase One - Study	Delivered 5/21	On sched
Phase Two - Concept Development	Pending	Contract/ Funding
Phase Three – Plan Development	Pending	Contract/ Funding

- Satisfied Congressional Staff interests and expectations regarding status of effort (IPRs)
- Networked key Stakeholders (Services and OSD Staff)
- Good relationship with (multiple) sponsors

Way Forward- Phase Two

Phase Two - Concept Development:

- Identify candidate training ranges (priority to INDOPACOM)
- Conduct range surveys that include EW tools/emitters, spectrum usage, and the training being done on site.
- Develop methodologies for conduct of surveys (for Department's use in future data collection).
- Identify potential customers and associated timelines for development
- Identify EW training and spectrum infrastructure needed now and into 2030.
  - Develop future spectrum operating characteristics.
  - Develop spectrum management and automation concept of operations.
  - Develop EW training concept (i.e., training audience, training objectives and training periodicity).

Way Forward- Phase Three

Phase Three - Plan Development:

- Deliver plans to implement the EW training and EMS capabilities required to mitigate training and spectrum risk, including establishment of a Joint EW Training Range(s).
  - Provide spectrum resource utilization policy recommendations.
  - Provide spectrum monitoring and automation policy and roadmap.
  - Provide EW training range improvement recommendations and roadmap.

Thank you!

Austin Branch

abranch2@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Managing & Mitigating Insider Risk

Mission Area Session

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Countering Insider Threat
(Moving to Insider Risk)

Adam Russell/ARLIS; Kelly Jones/ARLIS

Russell@umd.edu; kjones@arlis.umd.edu

Mission Area Objectives: Countering Insider Threat (Moving to Insider Risk)

- Think Differently: Conduct Social and Behavioral Science Research on Insider Threat
- Trusted Agent: An Independent Validation and Verification of Insider Threat and Vetting Technologies
- Educate: Outreach and Training on Insider Threat Prevention

Relationship to ARLIS's goals/story

- Leverage ARLIS's unique human domain expertise to **conduct and integrate** sociotechnical R&D and T&E to **deliver sociotechnical solutions** for emerging insider threat and personnel vetting needs

- Ties to other mission areas:
  - Insider threats to supply chains
  - Effects of malicious influence on insider threat events
  - Need for effective human/machine teaming for modeling, monitoring, and mitigating risks

- Builds data access and capabilities; builds T&E pipeline for emerging technologies

Insider Risk CONOPS

"Delivering and Sustaining an Uncompromised Workforce"

Major Subtasks

T0: Insider Risk Seminar Series (IRiSS)

Thinking Differently

T2: Insider Risk Hub Simulation

ICONS

SIMULATIONS • INSIGHTS • SOLUTIONS

T2: Crowdsourcing Insider Risk Forecasts

T2: Datasets for Modeling Insider Risk

T2: Identifying Risks of Radicalization

TRUST

T1: Defining TRUST & Research Questions

SELF

T3: Social media and "the self"

Insider Risk Project Constellation

Trusted Agent T&E

T4: Social Media Scraper Tools T&E

RISK →

T5: Remote Risk Assessment Tool T&E

Education

T6: Insider Risk College Course

IMS Vetting Lexicon SAF CDM

Big Wins (so far)

T0: Kick-off event

T1: Protocol in review

T3: Methods pre-registered

Thinking Differently

T2: Datasets for Modeling Insider Risk

T2: Insider Risk Hub Simulation

T2: 4 seedlings approved

T2: Identifying Risks of Radicalization

T2: Crowdsourcing Insider Risk Forecasts

Trusted Agent T&E

T4: Performer Companies engaged

RISK →

T5: Peer-review of protocol

Education

T6: Course registered for Summer 2021

Demonstrating tangible steps to delivering and sustaining an uncompromised workforce

Countering Insider Threat (Moving to Insider Risk)

- Sponsor: OUSD(I&S)
- Program Manager/Client: OUSD(I&S)
- Period of Performance: 06/2020 – 10/2021
- TRL of the work: 6.1 to 6.4
- Total Budget: $2.1 million
- Expenditures to date: $571,000

Team Members

- PI: Adam Russell, Kelly Jones
- ARLIS Team Members:
  - Current: Gabrielle Bonny, Breana Carter-Browne, Ruthanna Gordon, Meredith Hughes, Bernadette Jerome, Joe Kelly, Alexandra Maddox, Sara McConnell, Valerie Novak, Judy Phillipson, Harvey Rishikof, Anton Rytting, Jana Schwartz, Bill Stephens
    - Emeritus: Mike Bunting, Mike Maxwell, Polly O'Rourke
  - Graduate & Undergraduate Students: Shawn Janzen, Jordan Roberts
- Collaborating Institutions [if applicable]
  - UMD START: Bill Braniff, Devin Ellis, Mike Jensen, Barnett Koven, Katy Lindquist, Steve Sin
  - UMD BSOS: Long Doan, Ted Knight, Jean McGloin, Paige Miller
  - UMD Institute for Systems Research, Electrical & Computer Engineering: Carol Espy-Wilson, Cultivate Labs

Project Description: T3 - Online vs. Offline Selves

Goal: Survey existing research and gaps in our understanding of the relationship between social media representations and in-person selves; Translate and synthesize disparate strands of research

SWOT:

- Siloed research in various disciplines
- Lack social theories about how people choose to represent themselves online
- Lack focus on organization factors shaping online representations

Expected Outcome: Report on the systematic review of existing knowledge of social media representations with future research recommendations

Project Description: T3 - Online vs. Offline Selves

Success measures:

- Clarify when and how people use different impression management strategies online
- how these strategies may differ from offline strategies
- Better understanding of knowable unknowns

Expected Impact:

- Provide theoretical explanation for disparate findings
- Identify key unanswered questions that can be further examined

T3: Social media and "the self"

Overview: T3 - Online vs. Offline Selves

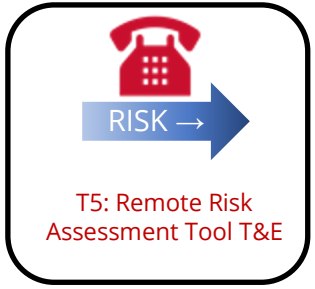
- Developed OSF preregistration of literature review methodology
- Literature review and report outline in progress
- Identifying potential directions for future research
- Anticipated draft of review write-up in summer

Project Description: T5 - Technology Evaluation of Voice Analytic tools

Goal: Provide independent evaluation of Clearspeed™ RRA®, a risk-assessment tool using audio recordings from a brief, automated interview

SWOT:

- Maintain independence of assessment;
- Examine RRA "flags" under additional experimental conditions; and
- Run complementary field- and experimental studies



Project Description: T5 - Technology Evaluation of Voice Analytic tools

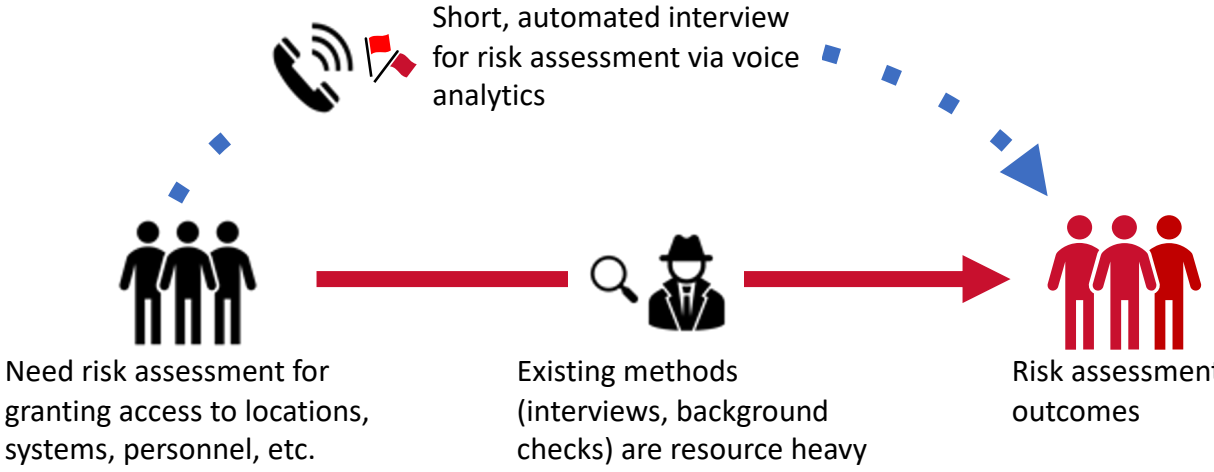
Expected Outcome: Support USG decision: How/Should they use the Clearspeed™ tool?

Success measures: Peer-supported research design; collect & communicate results well

Expected Impact: Save USG resources and/or maintaining quality of vetting decisions

Overview: T5 - Technology Evaluation of Voice Analytic tools

New technologies tout high-accuracy risk assessments via voice analytics: Are they worth the USG investment?



ARLIS Independent Evaluation

Does it really work? In the lab, in the field?

Does it work as well as (or better than) the status quo?

Are there unintended consequences of use (e.g., bias for/against irrelevant factors)?

Project Description: T6 – Insider Threat Summer Course

Goal: Establish an intensive undergrad and graduate summer course

SWOT: No course/program exists to educate college students in the holistic insider threat space

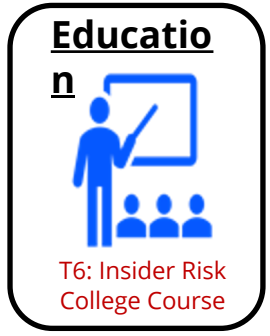
Expected Outcome: Educate the (potential) future workforce to the issue space of insider threat; pilot experiential learning via ICONS Simulation

Project Description: T6 – Insider Threat Summer Course

Success measures: Increase in the students' knowledge base about the insider threat issue space

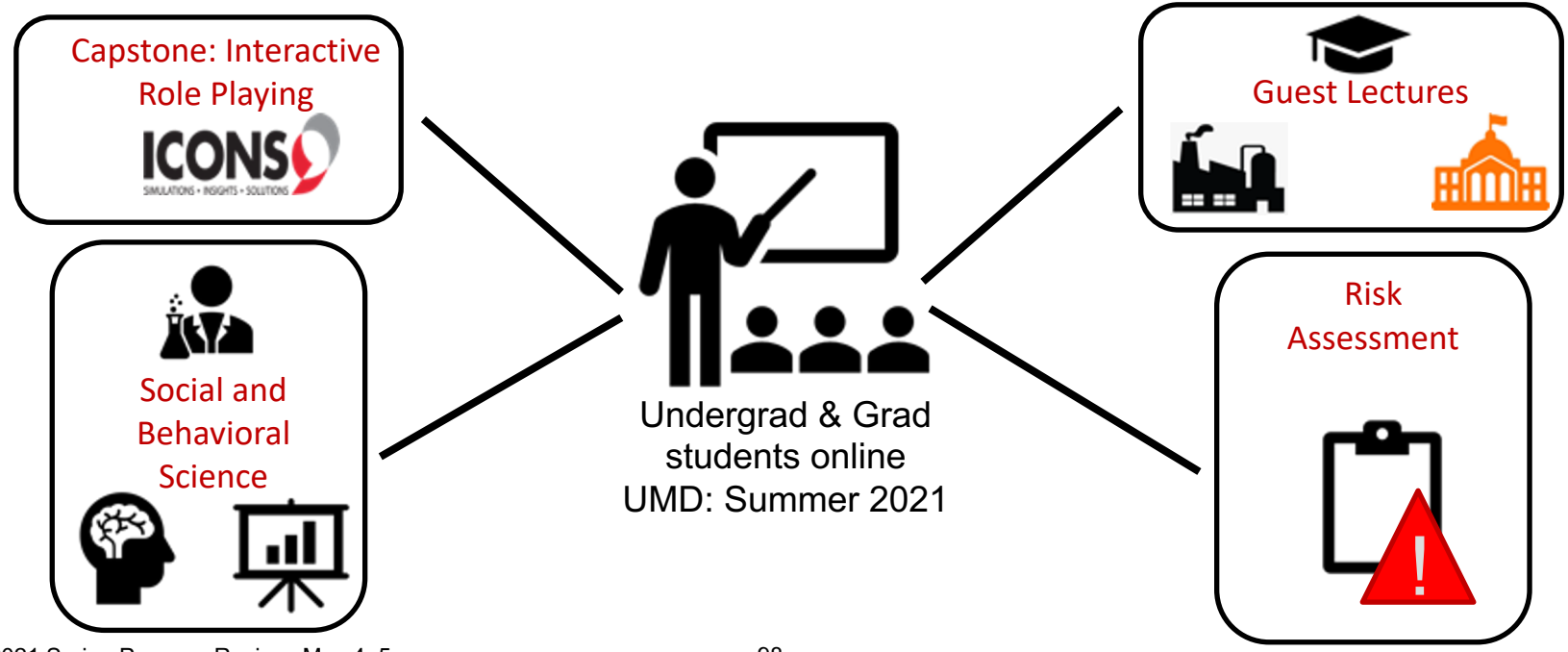
Expected Impact:

- Future national security workforce is
  - Exposed to current and future issue space of insider threat
  - Equipped with the knowledge base needed to identify, assess, and mitigate risk
  - Expose students to potential career paths



Overview - T6: Insider Threat Summer Course

- Establish an intensive summer course in Insider Threat education



Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
SBS Research (Tasks 1-3): Technical Reports on Research Results	End of POP	On sched
Personnel Vetting Tech T&E (Tasks 4-5): Technical Reports on Evaluation	End of POP	On sched
Summer Course (Task 6): Technical Report on Summer Program with Course Materials	End of POP	On sched

Project Risk Management

- Build up ARLIS infrastructure for handling CUI
- Identify and participated in Human Subjects Review protocols
- Performer teams for Tasks 4 – 5 might not want to compete – contingency plans to deliver evaluations
- COVID-19 mitigations: good communication & team building, online program management

Next Steps and Future Capabilities

Task	Activities & Milestones
T0: IRiSS	May – Industry Views; June – Hiring; July – Tools, Methods, & Tech; August – Managing Risk
T1: Insider TRUST	May – HRPO; June - SME interviews; July – Sept – write up
T2: ICONS	May – scenario programing; June – Aug – pilot in T6; Sept – write up
T2: C-SIFT for MInR	SME interviews, create question clusters, develop mock mission-centric dashboard
T2: CRA	Identify cases from PIRUS dataset, categorize risk indicators
T2: D-MInR	Identify datasets, design & develop matrix for cataloging
T3: Social Media & the Self	May – July – draft review; Aug – develop research questions; Sept – write up
T4: PAEI Scraper Tools T&E	May – June – data collection; July – Aug – analysis; Sept – write up
T5: RRA Tool T&E	May – HRPO; June – July – data collection; Aug – analysis; Sept – write up
T6: Summer Course	June – Aug – course runs; Sept – write up

Next Steps and Future Capabilities

- New ideas and whitepapers
  - Modeling the Academic Insider Risk Ecosystem
  - Demo of modeling capabilities in partnership with START
- Sponsor relationship, new/additional sponsors






the ThreatLab
Integrating Research Into Practice

MITRE

CERT

OPA | PERSEREC

The Center for Advanced Red Teaming
University at Albany

zoom

Seeking further sponsors & collaborators

LOCKHEED MARTIN

TU TOWSON UNIVERSITY

Thank you!

Kelly Jones and Adam Russell

kjones@arlis.umd.edu

arussell@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Understanding the Commercial Landscape for Detection

Dinesh Manocha & John Dickerson
Department of Computer Science
University of Maryland
dm@cs.umd.edu; john@cs.umd.edu

Understanding the Commercial Landscape for Detection

- Sponsor: OUSD(I&S)
- Program Manager: Stephanie Jaros
- Period of Performance: Dec 01, 2019 – May 31, 2021
- Total Budget: $200K (Expenditures to Date: $177K)
- Funding type: 6.6 (RDT&E Management Support)
- TRL of the work: 4
- Team: Dickerson, Manocha, one graduate student at UMD

Project Overview

- Goals: Explore Applications of AI Technologies to Improve Detection Efforts for Personnel Vetting and Insider Threat
- Approach: Evaluate AI and machine learning (ML) with prior datasets: automate and expedite processes
- Metrics: Identify the key areas where AI technologies can accelerate the process
- Transition Plan: Potential partners include DCSA, OUSD(I&S), and PERSEREC's Threat Lab to evaluate AI technology on real cases

Project 1:

Evaluate Challenges in an Operational Environment

State of the art evaluation

Visits and discussions: government labs & industry

- The Threat Lab; Monterey, CA
- Research Facilitation Laboratory, Army Analytics Group; Monterey, CA
- Lockheed Martin
- DCSA
- IBM Research
- DARPA
- Northrop Grumman
- Amazon

Insider Threat: State of the Art Evaluation

- Current AI technologies
- Open datasets and PAEI (publicly available electronic information)

PAEI Datasets and AI Technologies

PAEI Datasets

- Social media: text, videos, images, audio, etc.
- Public databases
- Credit reports, travel plans
- Court records, dark web, civic activity

AI Technologies: machine learning, computer vision, natural language processing (NLP), speech recognition, etc.

Detection & Data Gathering

- Current process relies heavily on human analysts and investigators on the ground
- Current process slow and expensive
- Generating labeled data is very costly, time consuming, and has privacy issues

Insider Threat: AI Technologies

- Current technologies rely on supervised algorithms
- Lack of labeled datasets is a major issue
- Current datasets may be biased
- Ensuring equitability in the outcomes from current tools is a challenge

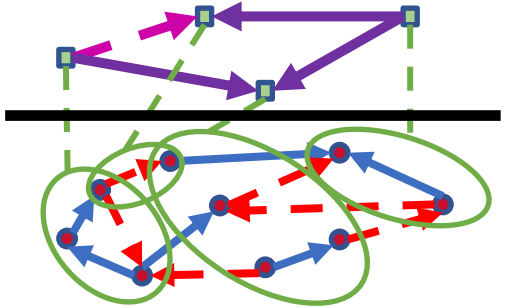
Insider Threat: Bias in AI Tools

- Acquisition planning
- Solicitation and selection
- Development
- Delivery
- Deployment, maintenance, and sustainment

Project 2:

New AI Methods for Continuous Vetting

Continuously Monitoring Hierarchical Networks



- Access to labeled, real-world (hierarchical) network data is not always possible
- Can we understand how membership in groups evolves over time?
- Track incremental changes in each individual's allegiance to multiple groups (potentially, or just binary allegiance/not to a single group)

Large-Scale Computational Methods for Node Labeling

- Hand-labeling approaches do not give complete results:
  - Limited by sparsity of chosen subgraphs
  - Require extensive human effort & knowledge

- Need computational approaches that can scale to the entire dataset – with uncertainties

PyTorch-BigGraph: Graph Embedding

Framework for placing nodes into a **low/medium-dimensional vector space**

Intuition: Nodes that communicate with similar nodes should have similar feature vectors

Algorithm: Push representations of neighbors towards each other, and push random pairs of nodes away from each other (negative sampling)

Our particular choices (for a real-world dataset of CDRs from Yemen):

- Maximize dot-product similarity
- 400-dimensional representations
- 1,000 uniform negative samples per batch
- Divide nodes into 5 subsets for distributed training

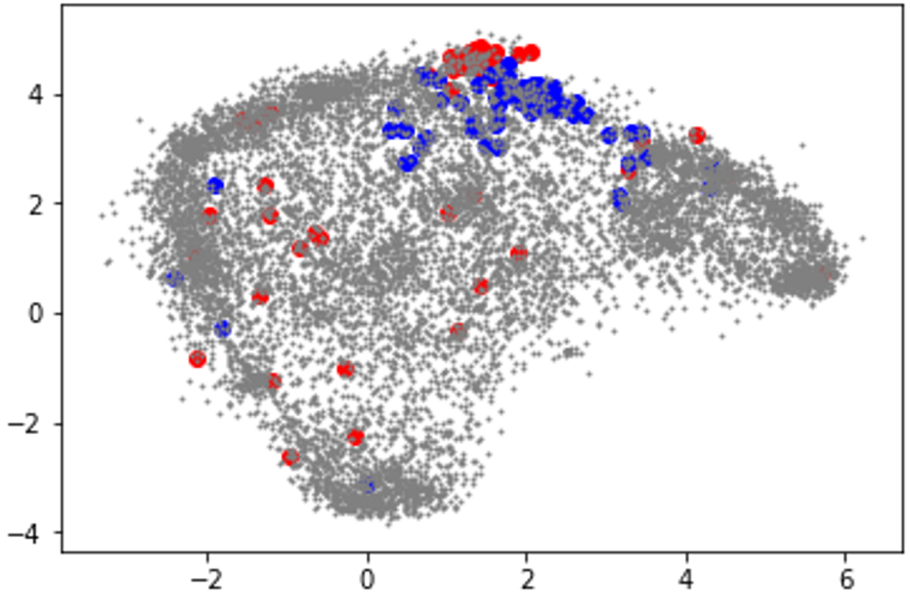
UMAP visualization of embeddings

2D visualization to confirm this embedding intuition

UMAP is a dimensionality-reduction technique (similar to more familiar t-SNE, but scales better to large graphs)

Experiment:

1. Sample 10,000 random background nodes, plus seeds
2. Run UMAP to project embeddings into two dimensions
3. Visualize



Even in 2D, seed red and blue nodes mostly cluster together with same color and away from opposite color

Continuous Diffusion of Influence: Hierarchical Networks

- Modeling continuous diffusion processes for more than one group (e.g., trustworthy, not trustworthy)
- Placement of scarce resources to learn (i) node membership, (ii) relationships between nodes, (iii) influence nodes' expressed beliefs
- Developed a model for hierarchical diffusion model (AAAI 2021)
- Expanding this to a continuous model, where network structure itself changes over time;
  - Application to time-varying datasets

Ongoing Work

- Work with stakeholders to evaluate the challenges. Apply these ideas to real-world dataset for anomalous behaviors
- Insider threat or Insider risk
  - Detection vs. Countering
  - NITTF: develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats

Relationship to ARLIS's Goals

- ARLIS: Applied Research Laboratory for Intelligence & Security
- Project leverages advances in ML and Artificial Intelligence to directly impact National Security needs.
- Specifically, will use AI technologies to improve detection efforts in Insider Threat Programs, Personnel Security and Vetting

Thank you

Dinesh Manocha
dm@cs.umd.edu
John Dickerson
john@cs.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Acquisition & Industrial Security

Mission Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Acquisition and Industrial Security

Thomas Hedberg, Jr., PhD, PE
Mission Lead, Acquisition and Industrial Security
thedberg@arlis.umd.edu

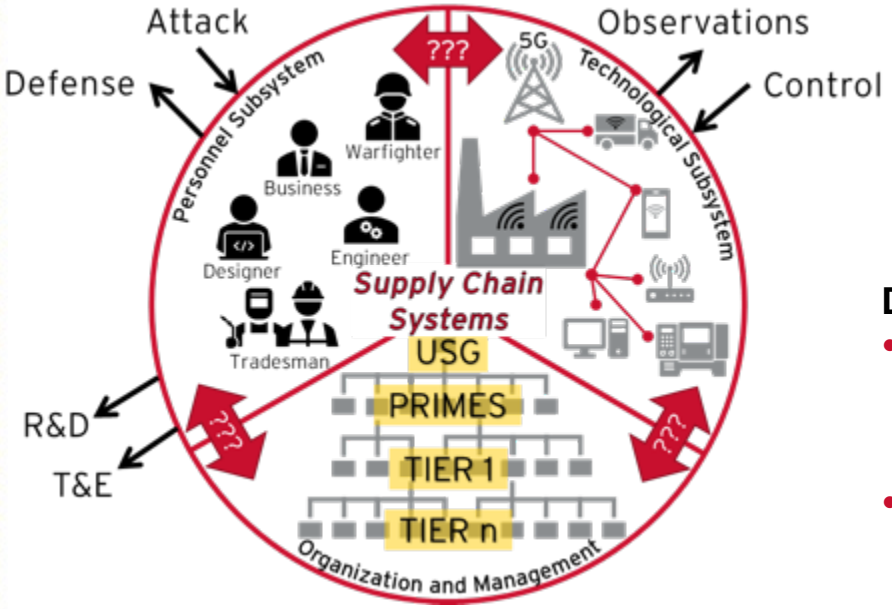
Mission Area Outline

- [10 min] Overview of the Mission
- [30 min] Critical Technologies Thrust: Wireless 5G Tech
- [30 min] Supply Chains Thrust

Mission Area Overview

Acquisition and Industrial Security (A&IS):

Uncompromised Delivery and Sustainment of Systems, Services, and People



Objective:

- Provide a capability for identifying and explaining what technologies and supply chains are too critical for the U.S. to lose --- but also, to determine what we can lose
  - Security
  - Resilience
  - Assurance
  - Blended Attack
  - Threat Vectors
  - Vulnerabilities

Discriminators:

- **People for X:** convergent set of experts in CS, Engr'ing, law, public policy, and social sciences
- **Data for X:** integrate and experiment with *all-source* data for cyber and physical systems
- **Analytics for X:** reusable cyber infrastructure for rapidly composing models and running scenario-based exercises

A&IS Definitions

- **acquisition security:** The safety or safeguarding, against some internal or external threat, of a directed, funded effort that provides a new, improved, or continuing material, weapon or information system, or service capability in response to an approved need of the Department of Defense.

- **industrial security:** The safety or safeguarding, against some internal or external threat, of machinery and engineering components used in manufacturing, supply-chain, and critical infrastructure operations.

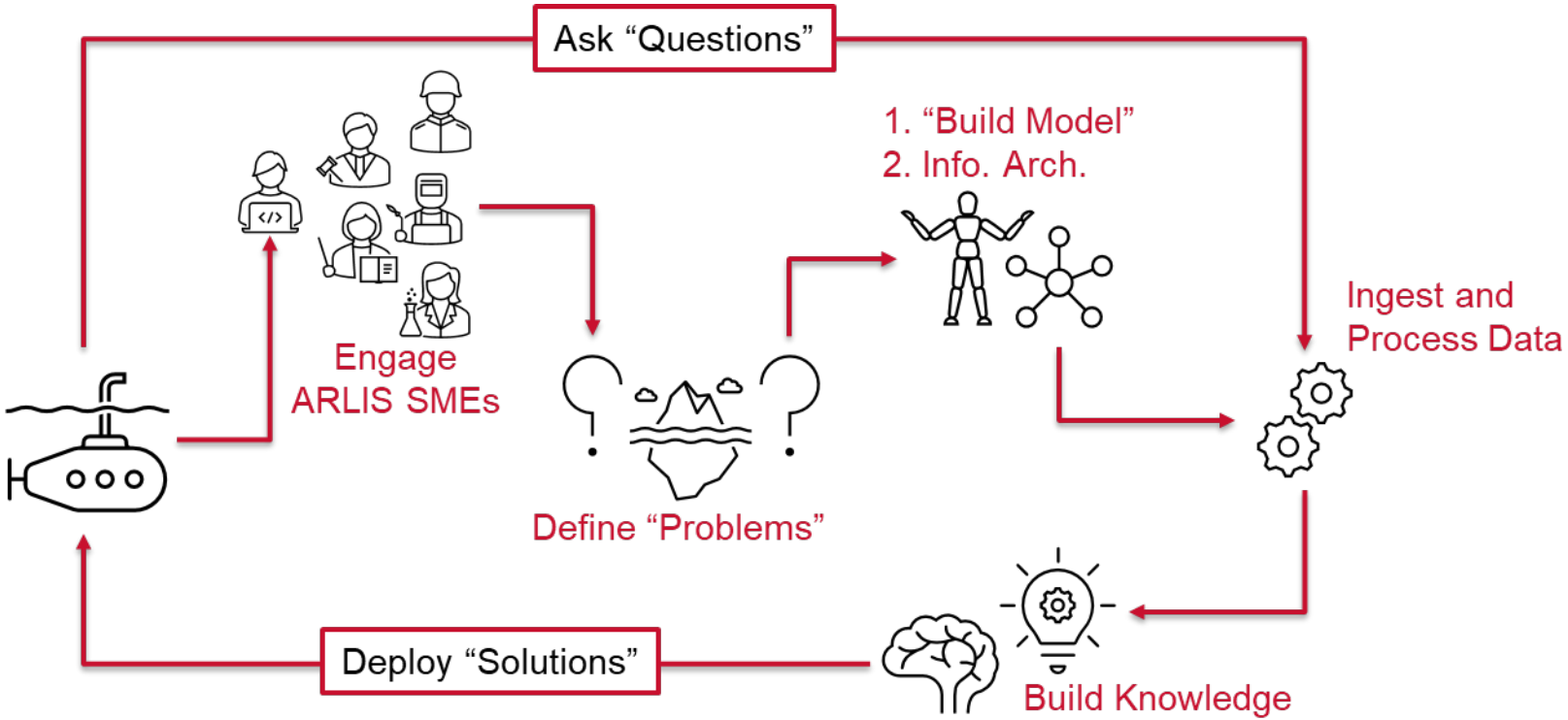
A&IS Relationship to ARLIS's Goals

- **Advanced Manufacturing:** Strengthen the DIB by expanding domestic manufacturing capabilities and security
- **National Security:** Join with like-minded democracies to develop and defend trusted critical supply chains and technology infrastructure
- **Cyber Strategy:** Must use a risk-management approach to mitigating vulnerabilities and raise the base level of cybersecurity across critical infrastructure
- **Counterintelligence:** Must prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of the deliveries from key U.S. supply chains

Acquisition and Industrial Security is a top priority for both the National and Economic security of the United States.

The Oracle of Intelligence and Security:

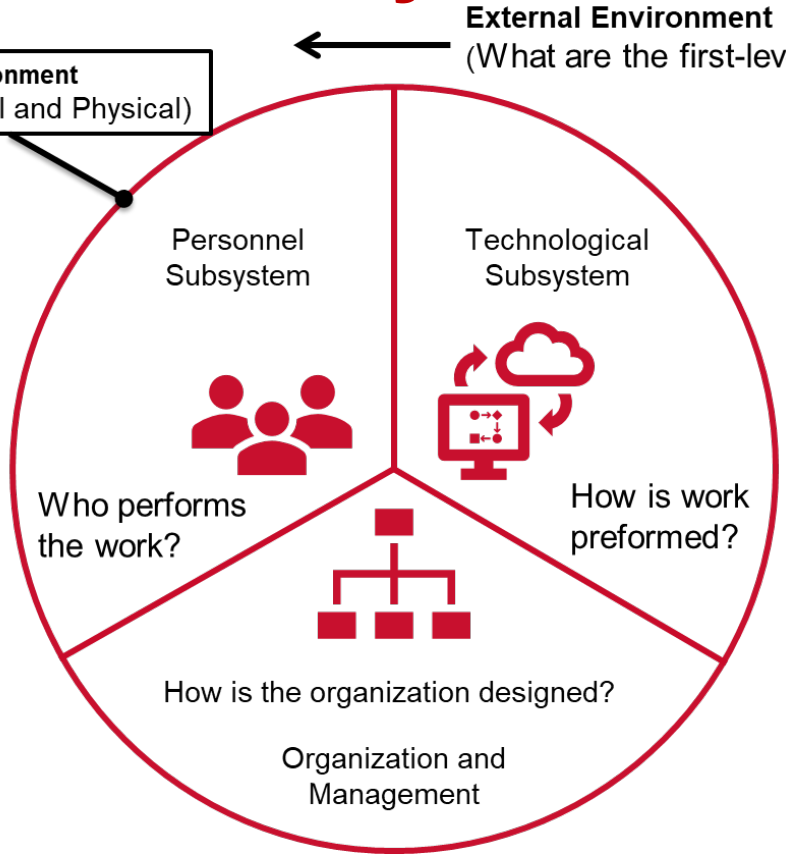
A Process Template



APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

UNIVERSITY OF MARYLAND

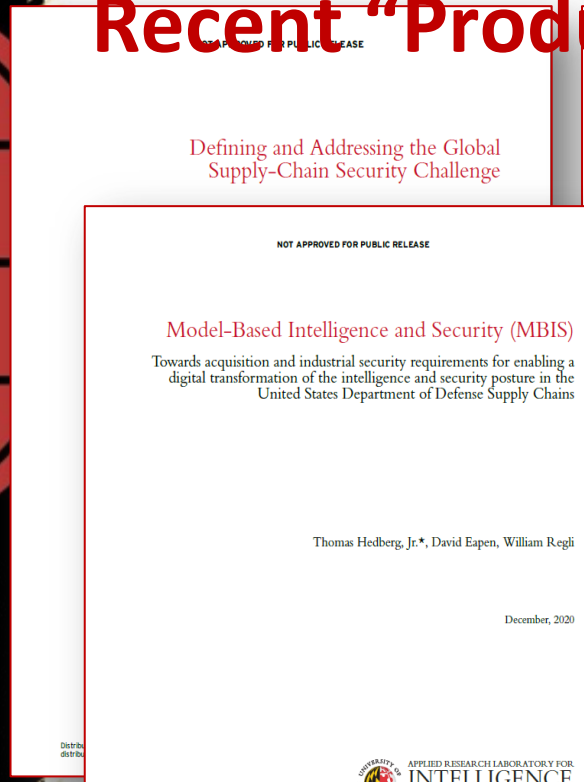
STS Analysis and Design



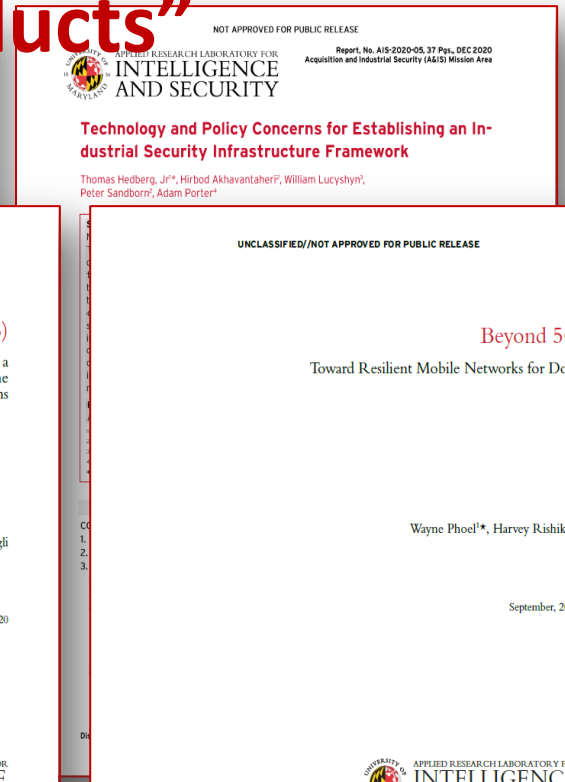
- **Theory of Joint Causation**
  - Subsystems are affected by causal events in the external environment and change in one subsystem causes changes in the others
- **Theory of Joint Optimization**
  - Maximization of overall work effectiveness requires joint design of subsystems toward the development of the best possible fit
- **Theory of Joint Design**
  - Be proactive, instead of reactive. Must consider subsystems jointly during design while considering objectives and requirements of subsystems

Kleiner, B. M. (2008). Macroergonomics: Work System Analysis and Design. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*(3), 461–467. https://doi.org/10.1518/001872008X288501

Recent "Products"



Defining and Addressing the Global Supply-Chain Security Challenge



NOT APPROVED FOR PUBLIC RELEASE

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Report, No. AIS-2020-05, 37 Pgs., DEC 2020
Acquisition and Industrial Security (A&IS) Mission Area

Technology and Policy Concerns for Establishing an Industrial Security Infrastructure Framework

Thomas Hedberg, Jr[1]*, Hirbod Akhavantaheri[2], William Lucyshyn[3], Peter Sandborn[3], Adam Porter[4]

NOT APPROVED FOR PUBLIC RELEASE

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Report, No. AIS-2020-04, 11 Pgs., DEC 2020
Acquisition and Industrial Security (A&IS) Mission Area

Foreign Investment Risk Management Through Continuously Updated Relational Networks

Joshua Giltinan[1], Madeline Diep[1], Adam Porter[1,2], Thomas Hedberg, Jr.[1]*

NOT APPROVED FOR PUBLIC RELEASE

Model-Based Intelligence and Security (MBIS)

Towards acquisition and industrial security requirements for enabling a digital transformation of the intelligence and security posture in the United States Department of Defense Supply Chains

Thomas Hedberg, Jr.*, David Eapen, William Regli

December, 2020

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

University of Maryland
Darryll J. Pines, President

Applied Research Laboratory of Intelligence and Security
William Regli, Executive Director

Distribution and releasability under review.

NOT APPROVED FOR PUBLIC RELEASE

UNCLASSIFIED//NOT APPROVED FOR PUBLIC RELEASE

Beyond 5G

Toward Resilient Mobile Networks for DoD

Wayne Phoel[1]*, Harvey Rishikof[1]

September, 2020

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

University of Maryland
Darryll J. Pines, President

Applied Research Laboratory of Intelligence and Security
William Regli, Executive Director

Distribution and releaseability to be determined.

UNCLASSIFIED//NOT APPROVED FOR PUBLIC RELEASE

NOT APPROVED FOR PUBLIC RELEASE

Modular Supply Chain Digital Twins

A Survey on the State of the Art in Digital Twins for Supply Chains and Manufacturing Systems

Timothy Sprock[1], Thomas Hedberg, Jr.[1]*, Joseph Balmain Rodgers[2], William J. Norris[2]

March, 2021

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

University of Maryland
Darryll J. Pines, President

Applied Research Laboratory of Intelligence and Security
William Regli, Executive Director

NOT APPROVED FOR PUBLIC RELEASE

Current Efforts ($5.81M)

- Acquisition Security: Security Framework and Hardware Testbed (OUSD(I&S), $1.27M)
- ARLIS Support to OUSD (R&E) 5G Initiatives (OUSD(R&E), $2.45M)
- Using Enterprise Network Models to Disrupt the Operations of Illicit Counterfeit Part Supply Chains for Critical Systems (NSF*)
- Acquisition Security: Supply-Chain Illumination and Protection (OUSD(I&S), $1.53M)
- Emerging Technologies, WMD, and Strategic Trade Controls (OUSD(A&S), $562K)

* ARLIS is in a support role for the A. James Clark School of Engineering

Critical Technology Thrust

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

5G Security Assessments and Support to DoD 5G Initiatives

Wayne Phoel
wphoel@arlis.umd.edu

Acquisition Security: Security Framework and Hardware Testbed

- **Sponsor:** OUSD(IS)
- **Program Manager:** Amanda McGlone
- **Period of Performance:** 19 May 2020– 30 September 2021 (requesting 6-month no-cost extension)
- **TRL of the work:** 4-5
- **Total Budget:** $1.27M
- **Expenditures to date:** $0.328M (not including encumbrances)
- **Team Members**:
  - PI: Wayne Phoel
  - Harvey Rishikof
  - Subawardee: Morgan State University

Leveraging Commercial 5G for DoD

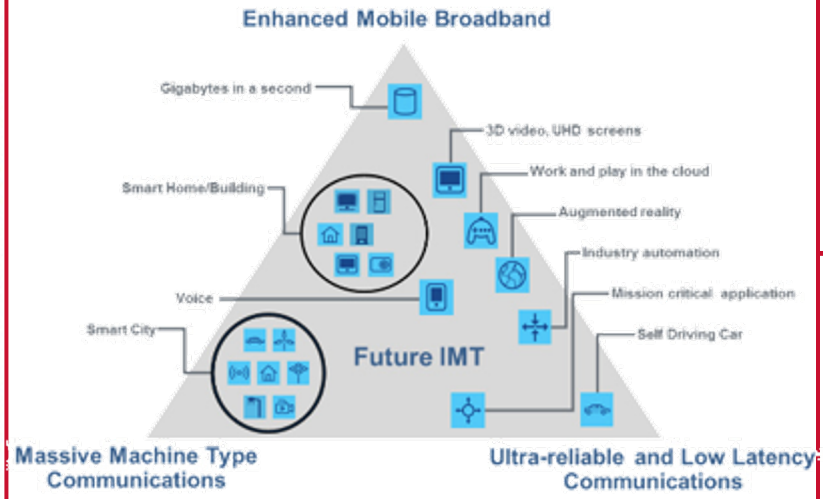
Commercial communications technology has outpaced DoD custom networks

China and Europe have overtaken U.S. leadership in standards and equipment

ARLIS focusing on how DoD can safely and reliably leverage commercial 5G

- Broad collaborations on DoD concerns and state of commercial technology
- In-depth analysis and experimentation of emerging architectures, vulnerabilities, and mitigations
- Growing leadership in future generations

5G Security Framework and Testbed



IMT: international Mobile Telecommunications

Objectives

- Refine security framework for 5G/Next-G
- Begin efforts to mitigate risks
- Test and evaluate 5G commercial systems for security issues and solutions

Project status

- Updated DoD 5G security framework
- Completed lab for over-the-air testing
- Received 5G hardware from CTIA
- Integrated IoT test bed zero-trust cloud environment

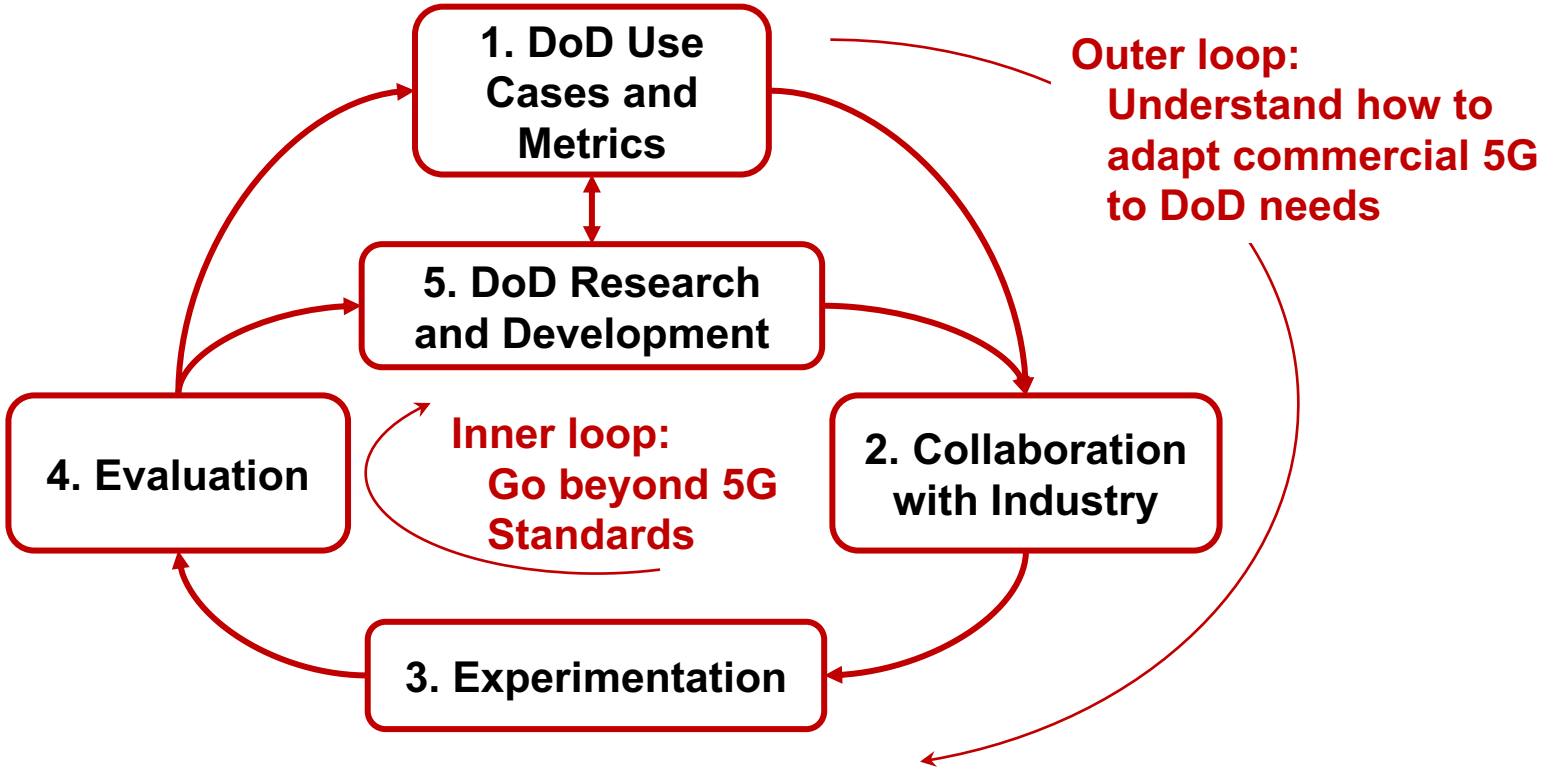
CTIA: Cellular Telecommunications Industry Association
IoT: Internet of Things

Security Framework and Current Work

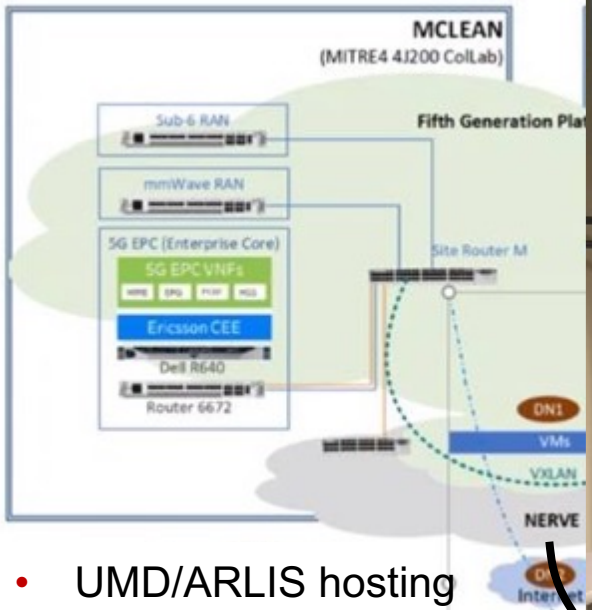
Requirements Mindset Mismatched to Commercial Evolution	OUSD(IS) OUSD(R&E)
Expectations of Open RAN Inconsistent with Development Timelines	OUSD(R&E)
"Operate Through" Conflated with "Zero Trust" Concept	OUSD(R&E)
Achieving DoD-Unique Security with 5G Components Still Notional	OUSD(IS) OUSD(R&E)
Network Traffic Analysis May Compromise Operations Security	
Uncertainty of Commercial IoT/mMTC Device Security for DoD	OUSD(IS)
5G Security May Fall Short if "Optional" Features Not Implemented	
Differing International Priorities, Economies, and Cultures	OUSD(IS)

RAN: Radio Access Network
IoT: Internet of Things
mMTC: massive Machine-Type Communications

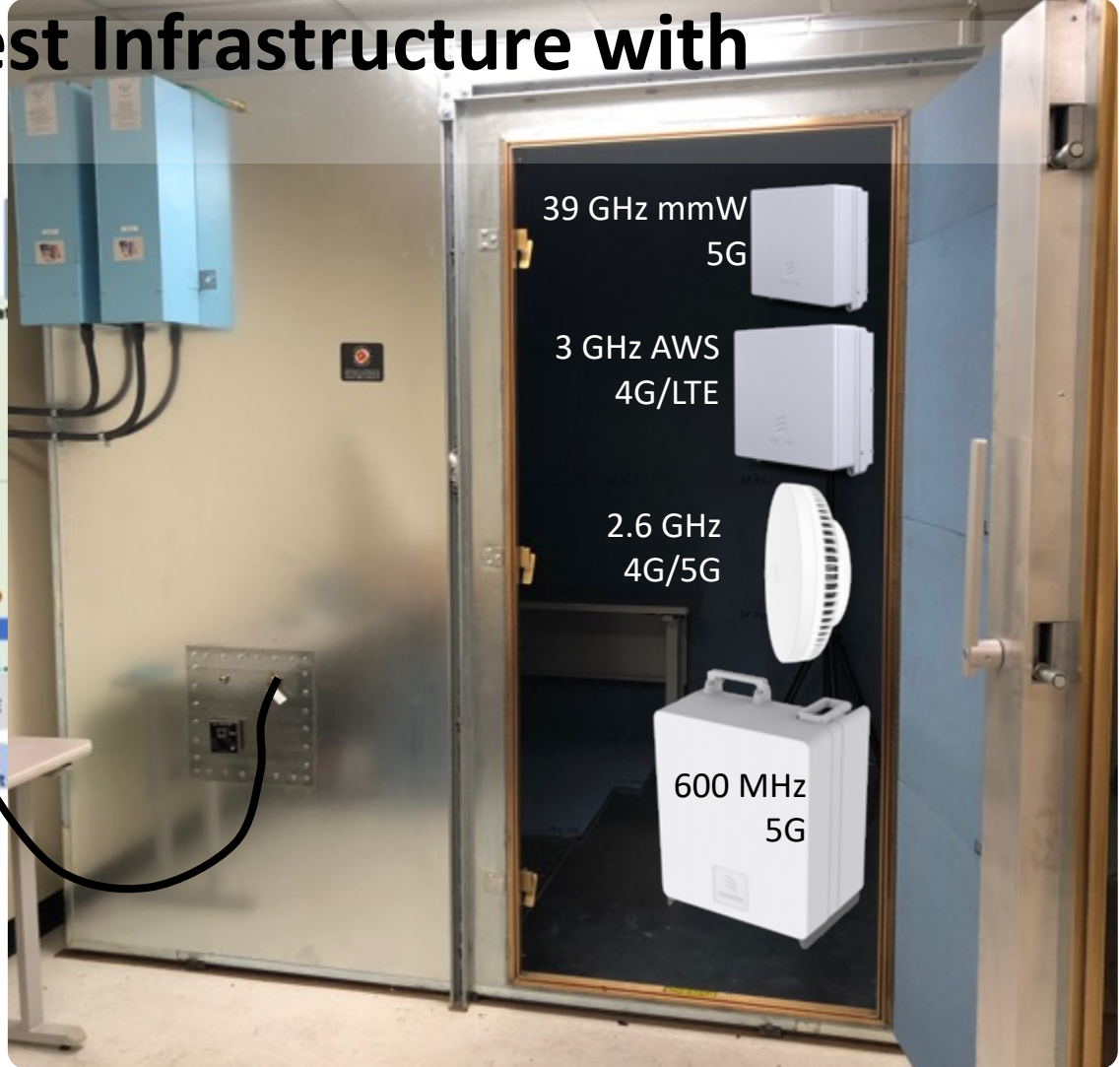
Effectively Integrating Commercial Tech



Collaboration Test Infrastructure with MITRE, Ericsson



- UMD/ARLIS hosting Ericsson equipment for over-the-air tests
- Connect to MITRE 5G network control software



Ongoing Collaborative Test Planning

- Initial test cases address 4G vulnerabilities
  - IMSI catching (i.e., Stingray)
  - Data encryption and integrity checks
- Evolving to consider cases of interest to DoD
  - CUI network “slice”
  - Security when roaming onto foreign network
- Network operators (AT&T, T-Mobile) providing systems-level guidance
- OEM (Ericsson) providing low-level capabilities and interfaces
- ARLIS, MITRE providing DoD perspectives and performing tests
- Virginia Tech assisting with test equipment, procedures

AT&T

ERICSSON

T-Mobile

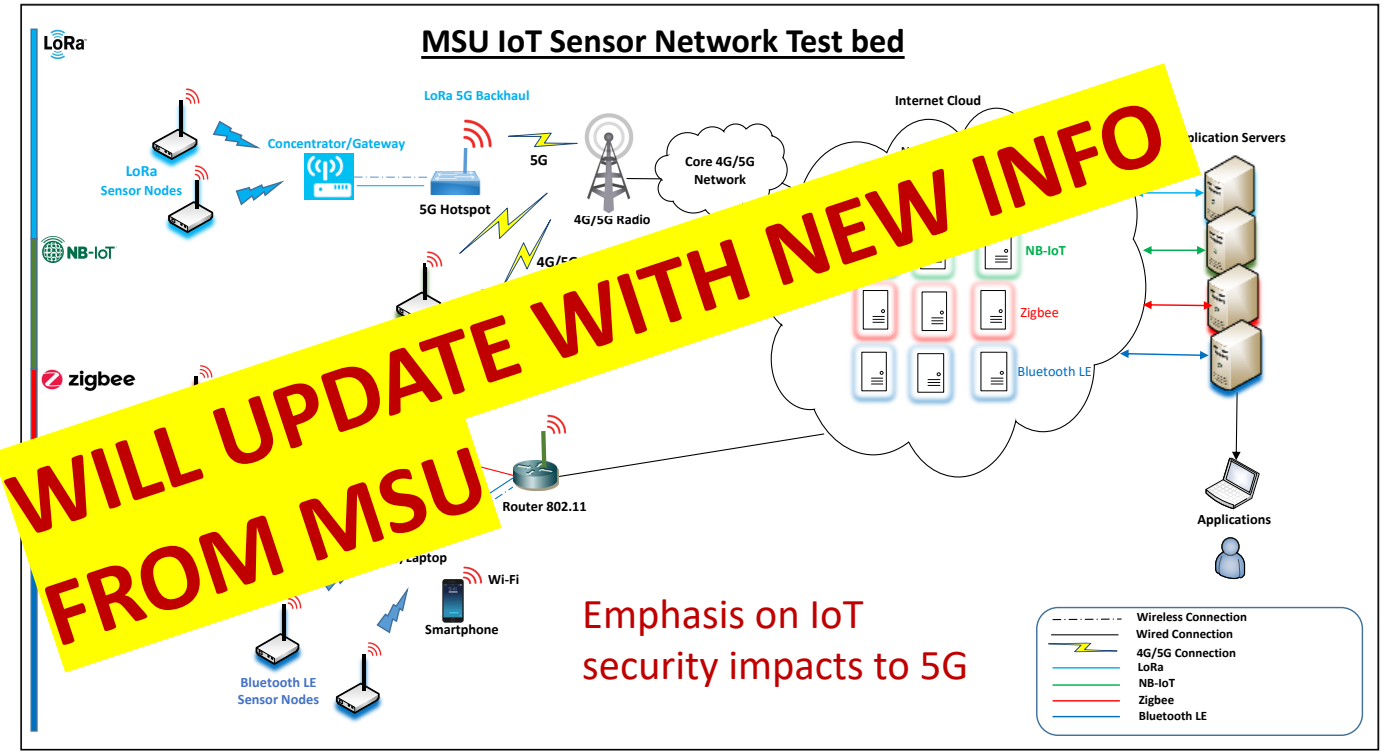
MITRE

VT

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

UNIVERSITY OF MARYLAND

Morgan State Merging IoT Assets with 5G Access and Zero Trust Cloud Architecture



WILL UPDATE WITH NEW INFO FROM MSU

Emphasis on IoT security impacts to 5G

MSU: Morgan State University
IoT: Internet of Things

NB: Narrow Band
LE: Low Energy

Big Wins

- Big Wins are on engagements with industry and government
  - ARLIS playing central role in CTIA 5G security industry test bed
  - Invited to present to ATIS Supply Chain Working Group, GSMA Security and Fraud Working Group
  - Invited to NSF Beyond 5G workshop; presented at OUSD(R&E) Innovate Beyond 5G Workshop
- Successful installation of RF-shielded enclosure and delivery of 5G radio hardware
- New program sponsorship from OUSD(R&E) 5G office

ATIS: Alliance for Telecommunications Industry Solutions
GSMA: Groupe Speciale Mobile Association

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Beyond 5G Security Workshop Report	6NOV2020	On sched
5G Hardware Test Plan	31MAY2021	Delayed
5G Security Workshop	TBD	Delayed

Concerns and Next Steps

- Hardware Test Plan delayed due to delayed equipment identification and coordination with industry partners
  - Issues seem to be resolved; actively prioritizing and coordinating test needs
  - Anticipate testing to begin late May
- Workshops delayed due to travel restrictions
  - Exploring alternative topics and/or classified teleconference capabilities

Support to OUSD(R&E) 5G Initiatives

- Sponsor: OUSD(R&E)
- Program Manager: Joseph Evans
- Period of Performance: 14 September 2020 – 13 March 2022
- TRL of the work: 3-4
- Total Budget: $2.4M
- Expenditures to date: $0.161M (not including encumbrances)
- Team Members:
  - PI: Wayne Phoel
  - Ted Woodward
  - Subawardee: Fraunhofer USA
  - Consultant: C3Comm Systems

DoD 5G Prototyping & Experimentation

- **Accelerate – Hasten DoD's adoption of 5G**
  - At-scale test facilities that enable rapid experimentation & dual-use application prototyping
  - Red/blue-teaming to identify and mitigate vulnerabilities
- **Operate Through – Ensure that US forces can operate through wherever and whenever we deploy**
  - Dynamic spectrum utilization
  - "Zero Trust" architectures
  - DoD-specific enhancements to commercial technology
- **Innovate – Enhance 5G technology and invest in future "Next G" technologies**
  - There is no finish line.

5G to Next G – Use Cases

Providing Strategic Guidance Supported by Hands-on Experience

- Subject matter expertise in
  - Program construction, metric definition, test and evaluation
  - Potential proposer capabilities
  - Multi-program interactions and orchestration (includes Spectrum Collaboration Challenge, Open 5G Challenge, OPS 5G)
- Developing working knowledge of 5G implementations
  - Working to obtain source code for fully deployable network core
  - Assessing application of zero-trust concepts to DoD 5G

Project Status

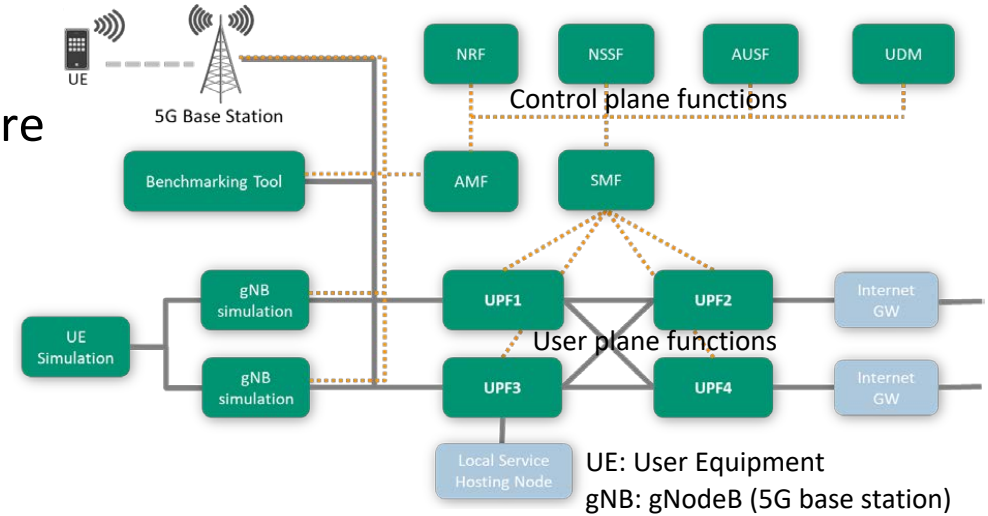
Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
5G Use Case Descriptions	21JAN2021	On sched
Inputs to Operate Through BAA	JAN-FEB2021	On sched
Zero-Trust Architecture Assessment	15MAY2021	Delayed

Concerns

- Prolonged subcontracting issues delayed network emulation development
  - Issues resolved and working to recover lost time
- Software licensing issue delayed access to network core software
  - Using subcontractor to license software; expected by mid-May
  - Identified alternative solutions as back-up/augmentation

Next Steps and Future Capabilities

- Continue subject-matter expertise contributions to Operate Through, Innovate Beyond 5G, ancillary efforts
- Stand up 5G network emulation and conduct initial experiments
  - Initial operational capability July
- Integrate network software with hardware testbed



Thank you!

Wayne Phoel

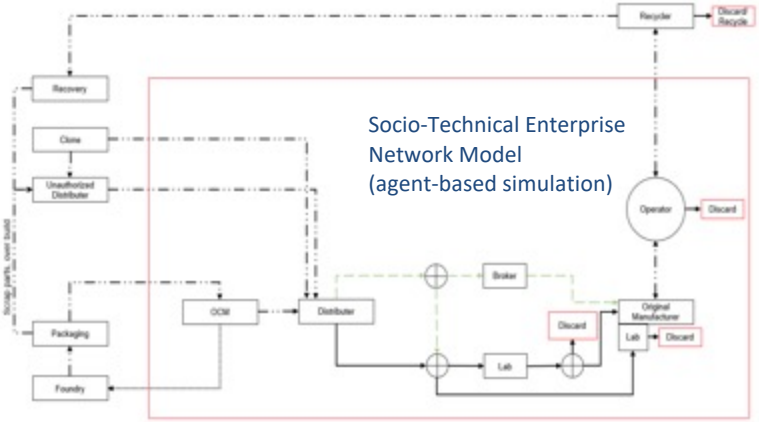
wphoel@arlis.umd.edu wphoel@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Supply Chain Thrust

Using Enterprise Network Models to Disrupt the Operations of Illicit Counterfeit Part Supply Chains for Critical Systems



POC: Prof. Peter Sandborn, sandborn@umd.edu

Upcoming Events:

- June 16 - Additive manufacturing compromise workshop
- August 5 – Electronic parts counterfeit network modeling workshop

- Develop methods of disrupting the counterfeit hardware network for critical systems guided by socio-technical network development and modeling.
  - The majority of the attention on the counterfeit electronic part problem has been on detection
  - Detection is important (and necessary), but represents treating the symptom not the cause
  - This program focuses on modeling counterfeit networks (for the purposes of disruption)
- The scope of our treatment is safety-, mission-, and infrastructure-critical systems
- Counterfeit hardware addressed includes:
  - Electronic parts
  - Additive manufacturing parts (or hybrids of additive and conventional manufacturing)

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Acquisition Security: Supply-Chain Illumination and Protection (SCIP)

Thomas Hedberg

thedberg@arlis.umd.edu

Acquisition Security: Supply-Chain Illumination and Protection (SCIP)

- Sponsor: OUSD(I&S)
- Program Manager/Client: Amanda McGlone
- Period of Performance: MAY 2020 thru SEP 2021
- TRL of the work: 2 to 5
- Total Budget: $1.53M
- Expenditures to date: $0.648M (not including encumbrances)
  - Requesting NCE

Team Members

- PI: Thomas Hedberg, PhD
- ARLIS Team Members:
  - David Eapen, Esq
  - Michael McGrath, PhD (Consultant)
  - Harvey Rishikof, Esq
  - Timothy Sprock, PhD
- UMD Team Members:
  - Prof. William Lucyshyn (SPP)
  - Prof. Adam Porter (CS)
  - Prof. Peter Sandborn (MechE)
  - Stephen Trimberger, PhD (ISR)
- Collaborating Institutions
  - Fraunhofer USA CESE (subawardee)

SCIP: Project Description

- **Goal:**
  - Integrate existing technology and policy frameworks to enable quickly generating problem-space definitions.
  - Develop modeling and simulation methods and modular environments to support rapid response to threats and vulnerabilities in supply chains and critical technologies
  - Define a standardized proving ground architecture that supports integrated TEVV of policy and technology solutions
- **SWOT**:
  - **Weakness:** Silos of excellence – lack of integrated views
  - **Threat:** Lots of exploratory, niche efforts being stood up – COVID driving lots of attention
  - **Opportunity:** McKinsey recommends using holistic and systematic analysis in making decisions on how and where to best deploy and maintain technologies and capabilities
  - **Opportunity:** Deliver Uncompromised says DoD needs better use of its existing resources to identify, protect, detect, respond to, and recover from network and supply chain threats

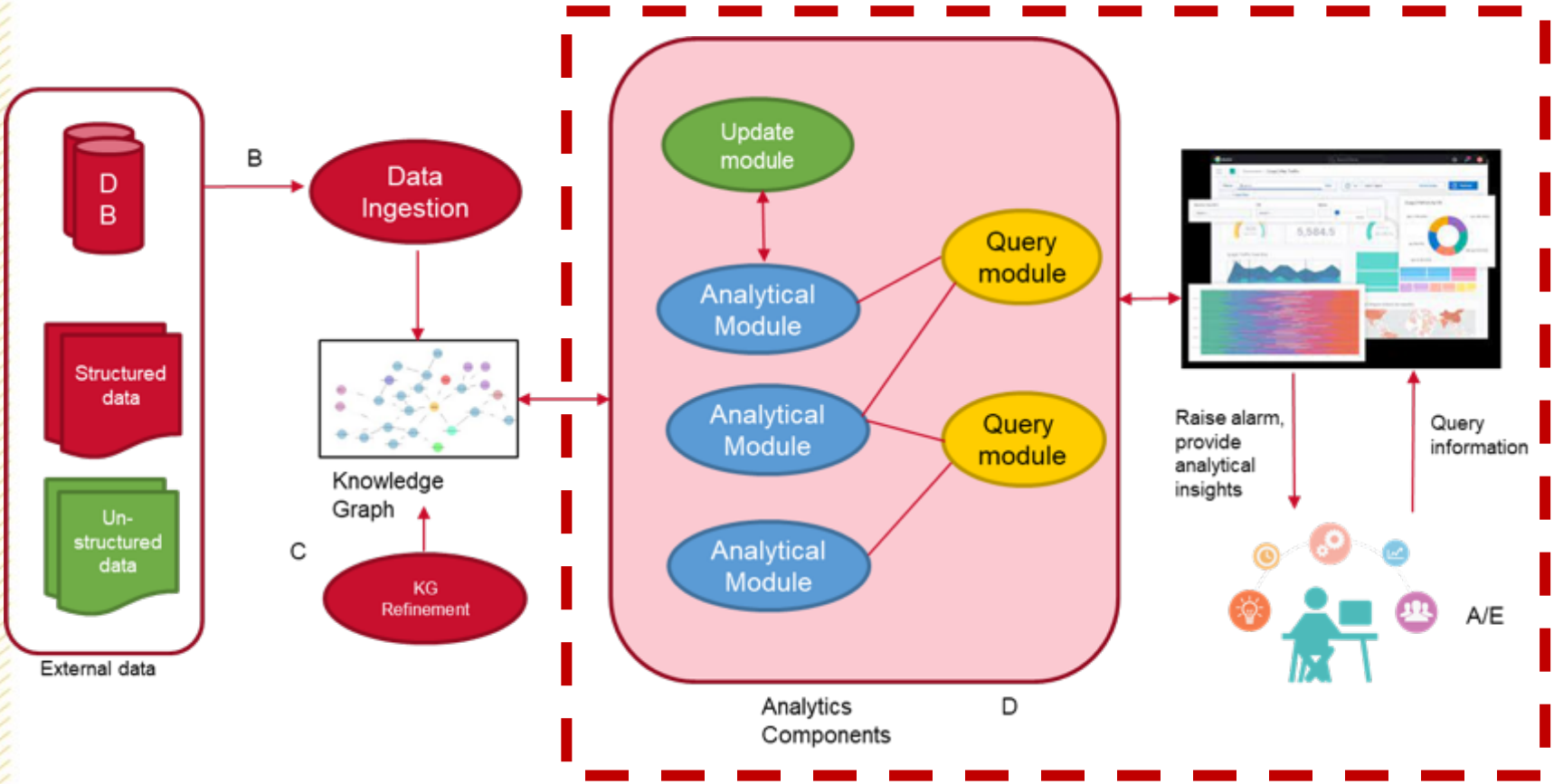
SCIP: Project Description, Cont.

- Expected Outcome:
  - ARLIS understands the risk that spans the threats and vulnerabilities related to people, technologies, organizational structures, policies and regulations
  - This work will enable the USG to quickly develop integrated risk profiles that give insight and enable actionable intelligence at the intersection of people, technology, and organization and policy

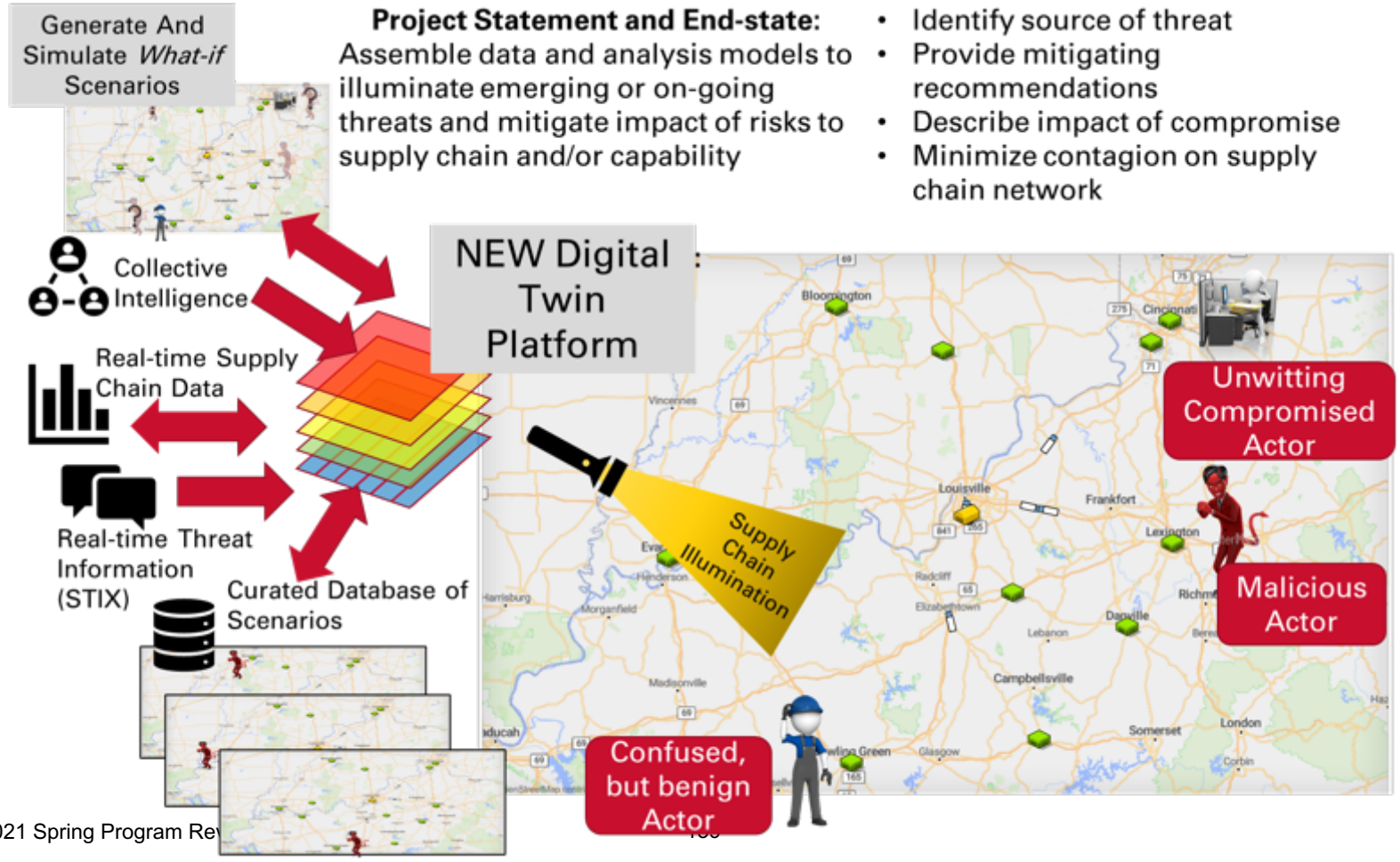
- Success Measures:
  - Functional use-case approach: (1) Trust and Traceability of Microelectronics; (2) Adversarial Capital and Behavior Economics; (3) Continuous Vetting; (4) Confidentiality, Integrity, and Availability Threat Mitigation, (5) Collective Intelligence

- Expected Impact:
  - Developing plan for transferring data-centric work products that increase visibility into performance, security, and stability of supply chains and critical technology deployments

TA1: Predictive Analytics Framework for SCRM



TA2: Modular Supply Chain Digital Twins



Project Statement and End-state:
Assemble data and analysis models to illuminate emerging or on-going threats and mitigate impact of risks to supply chain and/or capability

- Identify source of threat
- Provide mitigating recommendations
- Describe impact of compromise
- Minimize contagion on supply chain network

SCIP: Project Status

Key Deliverables/ Insights / Activities	Status	R/Y/G
ST1: Technical report documenting the government and public datasets available for SCRM forecasting	COMPLETE	G
ST1: Technical report documenting the current landscape of AI algorithms, training models, and implementations for SCRM forecasting	COMPLETE	G
ST1: Demonstration and technical report documenting prototype predictive analytics capability for SCRM forecasting	WIP	G
ST1: Demonstration and technical report documenting a dashboard tool for SCRM forecasting	SEP2021	G

SCIP: Project Status

Key Deliverables/ Insights / Activities	Status	R/Y/G
ST2: Technical report introducing the concepts of model-based enterprise, digital thread, and digital twin in the context of the IC	COMPLETE	G
ST2: Technical report documenting the stakeholder needs, use cases, and requirements	COMPLETE	G
ST2: Technical report documenting needed, existing, and missing testing capabilities and information systems	COMPLETE	G
ST2: Technical report documenting the architecture and systems models	WIP	G
ST2: Demonstration and technical report documenting the recommended practices for deploying digital twins with the architecture	SEP2021	G
On-demand responses to sponsor questions related to supply-chain illumination, observation, and protection	WIP	G

Project Risk Assessment

- **PM:** Initially decomposed the work breakdown structure too much and the deliverables may lack context
  - **Mitigation:** Proposing to combine some deliverables to ensure appropriate context is provided to the stakeholder; all work will still be done, but delivered in larger packages
- **Tech:** Lack of data accessibility and availability
  - **Mitigation:** R&D technology and policy for archiving and sharing curated data sets. R&D surrogate data generation for helping fill gaps in operational scenarios. Get really good at uncertainty quantification.
- **Tech:** Lack of problem model-ability
  - **Mitigation:** R&D methods for combining formal models, informal models, and human intervention into a heterogeneous analysis workflow.
- **HR:** Lack of skilled workforce (e.g., modelers, researchers)
  - **Mitigation:** R&D a framework enables curated reusable scenarios that can scale multiple problem sets and enable learning from the past.
- **Tech**: Lack of scalability
  - **Mitigation:** Assist the stakeholders and researchers with getting comfortable in using the 80% solution… reusing a curated model that doesn't exactly fit the current scenario but produces enough knowledge for deciding a course of action.

Next Steps and Future Capabilities

- Transition goals
  - Demonstrate the connections between the CTP/5G and Supply Chain thrusts of the mission
  - Operationalize reusable modeling and simulation capabilities for stakeholder engagement
  - Enable integration with Cognitive Security Proving Ground and eventual Insider-Risk models
- New ideas and whitepapers
  - Operational Technology (OT) Research → Services see this as a big gap
  - Response-Team Rolodex / Data Observatories (working with the Cyber Infrastructure team)
- Sponsor relationship opportunities (and potential funding on its way)
  - Services (USN, USAF), DCSA, DLA, DARPA, NSA, DOC/NIST

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Emerging Technologies, WMD, and Trade Controls

Nancy Gallagher, CISSM Director

ngallag@umd.edu

Emerging Technologies, WMD, and Trade Controls

- **Sponsor:** OUSD(Acquisition & Sustainment)
- **Program Manager/Client:** James Stokes
- **Period of Performance:** October 1, 2020-September 29, 2021
- **TRL of the work:** N/A
- **Total Budget:** $561,739
- **Expenditures to date:** $ 409,932
- **Team Members**:
  - Nancy Gallagher
  - Jonas Siegel
  - Andrea Viski (STRI, Phase One)
  - Lindsay Rand
  - Francesca Perry
  - Devin Entrikin
  - Naoko Aoki
  - CJ Horton

Project Description

Goal: To conduct research and provide expertise related to governance mechanisms that can minimize risks from proliferation of weapons of mass destruction (WMD) and emerging technologies.

SWOT: Many current policy efforts to manage emerging technologies are overly broad. They ignore technology-specific traits which affect the feasibility and desirability of getting stakeholder agreement on governance mechanisms to minimize security risks without unduly harming technology innovation and economic competitiveness.

Project Description Cont.

Expected Outcome: This research will contribute towards furthering dialogue on technology governance through deliverables from three main phases of work.

- Phase 1 will survey stakeholder viewpoints on technology policymaking across private industry and government agencies, with emphasis on response to different policy approaches towards emerging technology governance.
- Phase 2 will analyze the technology sectors and identify technology-specific development characteristics for 5 emerging technologies.
- Phase 3 will compare findings across the technologies to present key trends of emerging technology development and survey a wide range of policy mechanisms that could be used to meet different policy objectives.

Success measures: The research will be successful if it improves decision-making about management of risks associated with proliferation of WMD and emerging technology in general and/or on the specific technologies analyzed.

Expected Impact: This work will promote a more nuanced understanding of emerging technology governance to promote agreement on technology-specific policy mechanisms that can reduce security risks without unduly harming technological innovation or economic competiveness.

Project Overview – Phase 1

Phase 1: Stakeholder motivation/objective analysis (in partnership with Strategic Trade Research Institute)

Phase 1 Objective:

- Meet with stakeholders across sectors to identify driving strategic objectives and views on technology governance.

Phase 1 Status and Deliverables:

- Status: Complete
- Deliverable: Report on stakeholder perspectives in the case of artificial intelligence and notes for conferences/meetings with stakeholders.

Project Overview – Phase 2

Phase 2: Technology Sector Analysis

- Computer vision
- Quantum Computing
- Positioning, Navigation, and Timing (PNT)
- Quantum Sensing
- Hypersonics

Phase 2 Objective:

- Map five emerging technology sectors to identify key features including stage of development, stakeholders, geographic distribution, and extent of international cooperation/financing.

Phase 2 Status and Deliverables:

- Status: In progress (3/5 complete)
- Deliverable: Reports on the quantum computing, computer vision, and PNT complete. Reports for quantum sensing and hypersonics in progress.

Project Overview – Phase 3

Phase 3: Policy Mechanism Analysis

Phase 3 Objective:

- Facilitate agreement among USG entities and other stakeholders on policy mechanisms to reduce security risks associated with different types of emerging technologies.

Phase 3 Status and Deliverables:

- Status: In progress
- Deliverable: Report on stakeholder views of feasible and desirable policy mechanisms to manage risks and tradeoffs across five technology sectors.

Relationship to ARLIS's goals/story

- This project requires expertise in numerous emerging technologies where UMD is at the cutting edge of research.
- It demands deep knowledge of existing and potential future governance mechanisms that can be used to reduce security risks without unduly harming technology innovation or economic competiveness, issues at the heart of CISSM's research agenda.
- It benefits from the understanding of different stakeholder perspectives which come from being at a land-grant university that
  - is a trusted partner to key USG agencies,
  - has a mission to foster technological innovation and economic growth for the state of Maryland, and
  - that supports professional interactions with academics from countries whose cooperation would be needed for effective governance of emerging technologies.

Big Wins (so far)

- The completion of Phase 1 and part of Phase 2 (so far, 3 of the five technologies) has provided significant insight into the quantum computing, computer vision, and positioning, navigation, and timing (PNT) sectors.

Project Status

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Phase 1 – Stakeholder survey	Complete	On sched
Phase 2 – Technology 1,2,3, analysis	Complete	On sched
Phase 2 – Technology 4 and 5 analysis	In progress	On sched.
Phase 3 – Policy Mechanisms analysis	In progress	On sched.

Project Risk Assessment

- The main impact of COVID-19 has been the cancellation of in-person events which would have allowed for more discussions with private and public stakeholders.
- We have compensated by doing some network-building events by Zoom and by shifting the focus of the project from network-building to research and policy engagement.

Next Steps and Future Capabilities

- Activities and milestones ahead:
  - Complete Phase 2 Technology Analyses
    - Hypersonic Technologies Analysis
    - Quantum Sensing Analysis
  - Complete Phase 3 Policy Mechanism Report

Thank you!

Nancy Gallagher
ngallag@umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Thank you!

Mission Area Lead: Thomas Hedberg, Jr., PhD, PE
thedberg@arlis.umd.edu

5G Tech Lead: Wayne Phoel, PhD
wphoel@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

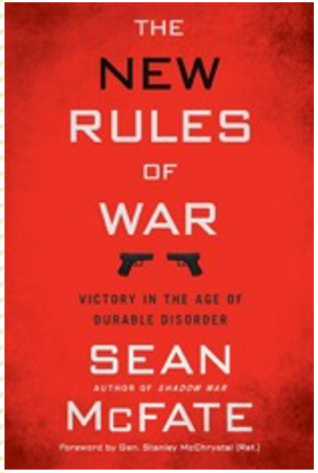
Augmented Collective Intelligence

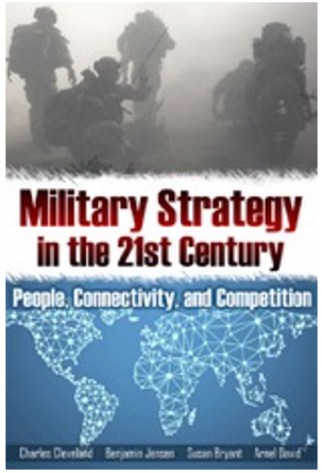
Mission Area Session

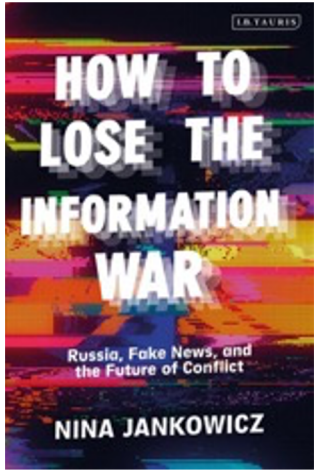
APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

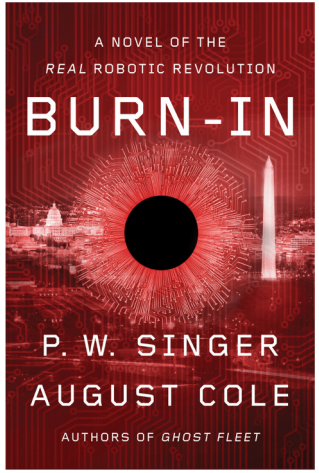
Augmented Collective Intelligence

Today's threats increasingly arise from interconnected sociotechnical networks









"These are problems which involve dealing simultaneously with a sizable number of factors which are interrelated into an organic whole. **They are all, in the language here proposed, problems of organized complexity** ...too complicated to yield to the old nineteenth-century techniques which were so dramatically successful on **two-, three-, or four-variable problems of simplicity**…[and] cannot be handled with the statistical techniques so effective in describing average behavior in problems of **disorganized complexity**."

- Warren Weaver, "Science and Complexity" (1947)

Problems of Organized Complexity

- There is a lack of clean, historical data to build comprehensive models;
- The future may have little to no resemblance to the past;
- There are numerous variables and outcomes to take into account and/or causal factors that are complex and not easy to measure;
- Regular streams of new information must be weighed and considered;
- There's a possibility of surprise events that likely wouldn't be found in data patterns.

Problems of organized complexity are becoming the norm, not the exception

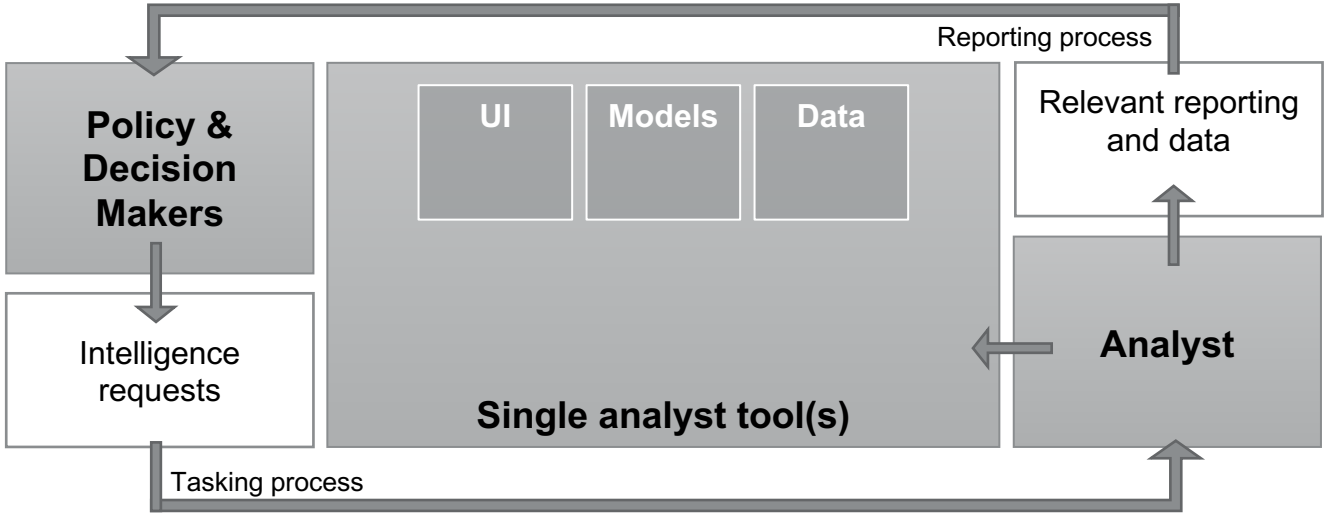
Collective Intelligence

- A **property of groups that emerges** from synergies among data-information-knowledge, software-hardware, and individuals (those with new insights as well as recognized authorities) that enables **just-in-time knowledge for better decisions** than these three elements acting alone.[1]

Can we augment our "collective intelligence" for competitive advantage?

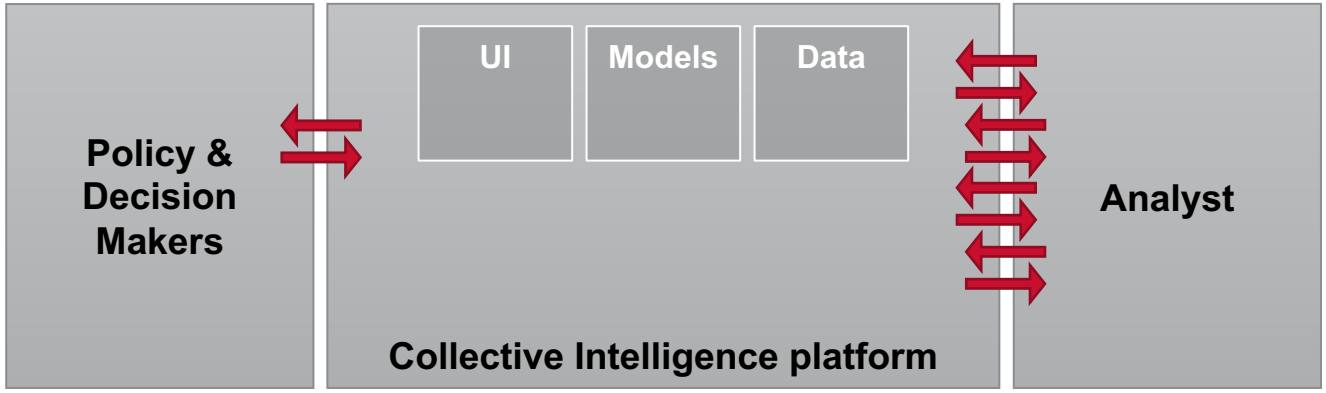
[1] https://dl.acm.org/doi/pdf/10.1145/3368986

Today's intelligence process



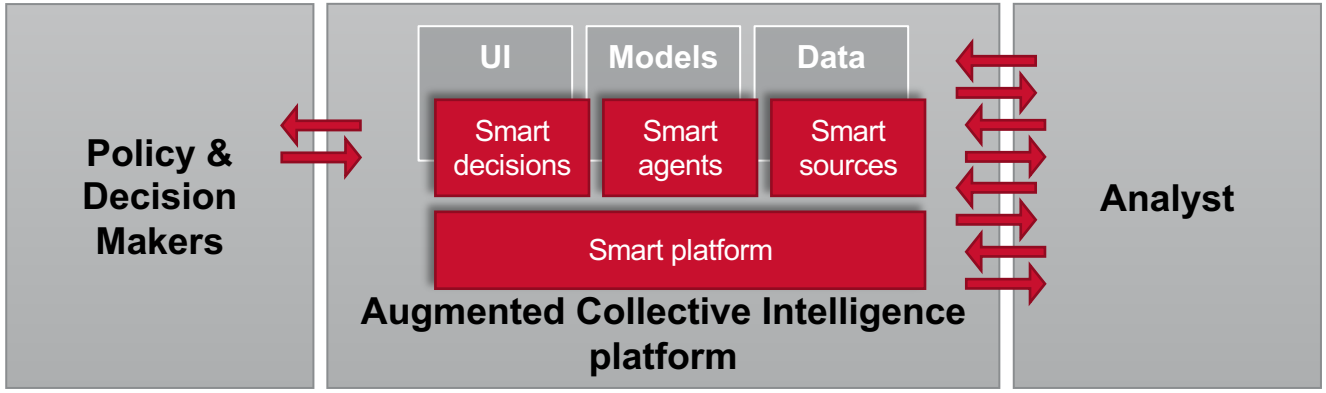
Today's processes don't fully leverage potential synergies

Collective Intelligence efforts have demonstrated value



Increases speed, scale, and accuracy of inputs

Augmented Collective Intelligence augments our human workforce with machine intelligences



Goal: increase speed, scale, and accuracy of decision-making

Crowdsourced Security & Intelligence Forecasting Tool

CSIFT for Supply Chain Security

CSIFT for Supply Chain Security

- Sponsor: OUSD(I&S)
- Program Manager/Client: OUSD(I&S)
- Period of Performance: 12/15/20 – 12/14/21
- TRL of the work: 7
- Total Budget (+ Expenditures to Date): $750,000 ($14,342)
- Team Members (co-PIs, subawardees):
  - PI Jana Schwartz
  - Adam Russell, Tom Hedberg + A&IS team, Ruthanna Gordon, Joe Kelly
  - Subawardee: Cultivate Labs

The IC has demonstrated that crowdsourced forecasting can create decision advantage

The CSIFT platform is inspired both by this research and a track record of real-world use to leverage human judgment and fill gaps where traditional data-driven models don't capture all relevant information.

KEY OUTCOMES FROM PRIOR WORK

- Aggregated probabilistic judgments of a large, reasonably **well-informed population can outperform "experts"**;
- With training, practice, and collaboration, **people can become more accurate forecasters over time**; and
- Mathematical aggregation of probabilistic judgments made by many individuals — based on performance, expertise, and psychoanalytic profiles — **can increase consensus forecast accuracy by as much as 30%**.

"The actual proves the possible"

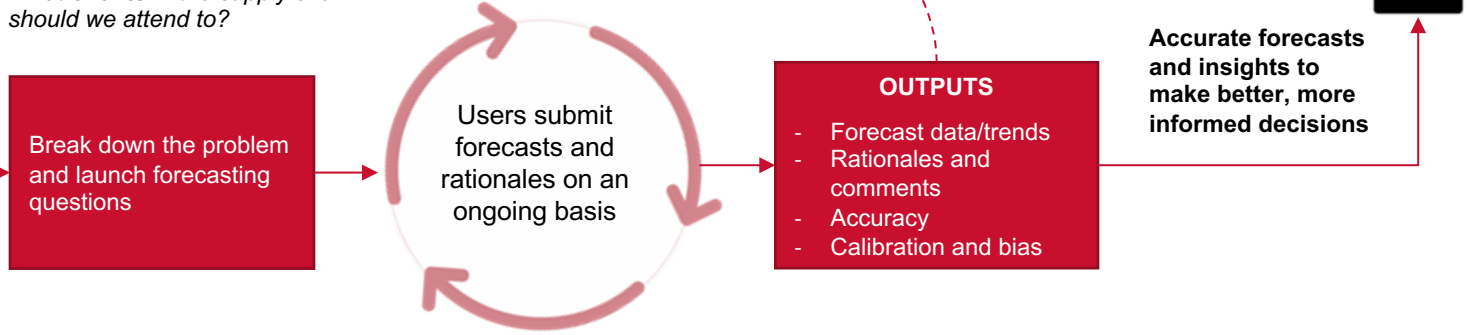
APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

How can CSIFT work in a Supply Chain context?

CSIFT, leveraging our forecasting and analysis platform, can facilitate the collection and measurement of forecasts from a large, diverse population who have perspectives on relevant events:

Decision maker: *There is an ever-expanding list of threats to protect against. Prioritizing where to focus limited resources is increasingly difficult.*

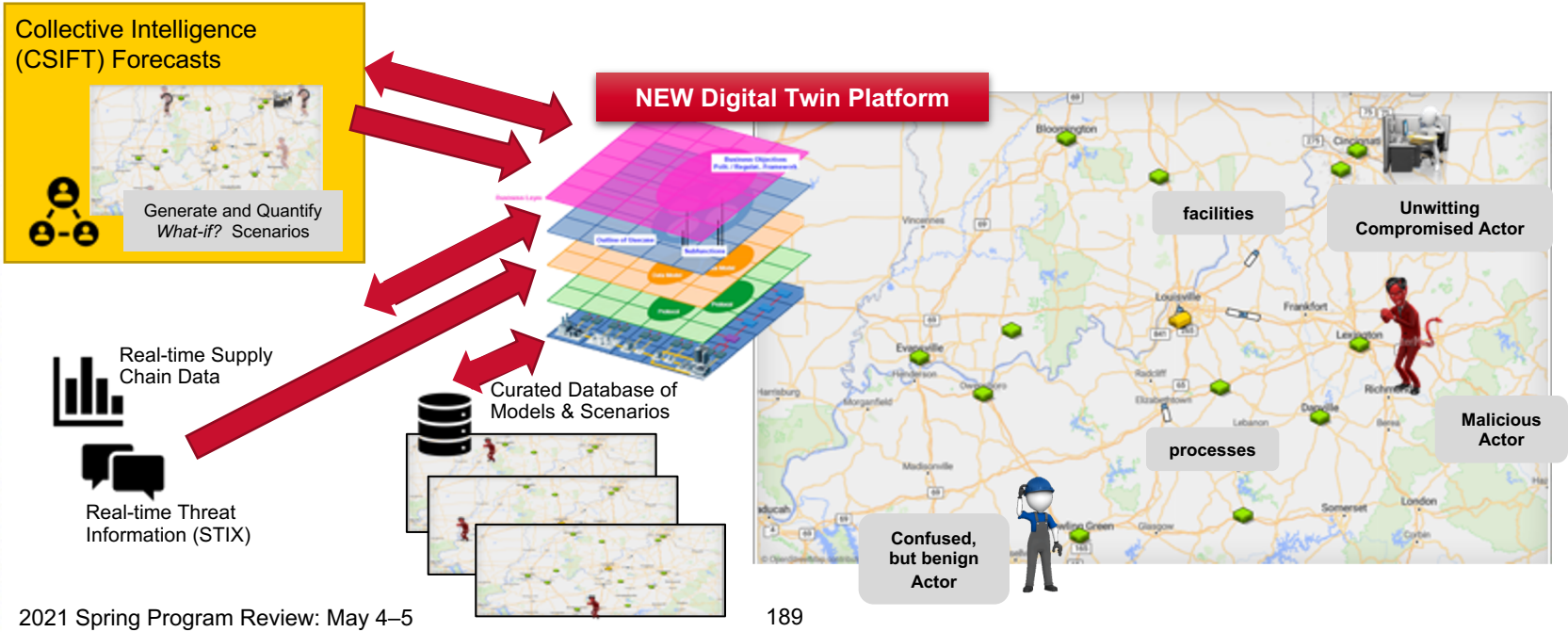
- *Are attacks more likely on **major infrastructure elements** or end-point devices?*
- *What **events** in the supply chain should we attend to?*



To understand an overarching issue, decompose into possible outcomes, and ask signaling questions.

CSIFT provides one piece of the integrated supply chain security solution

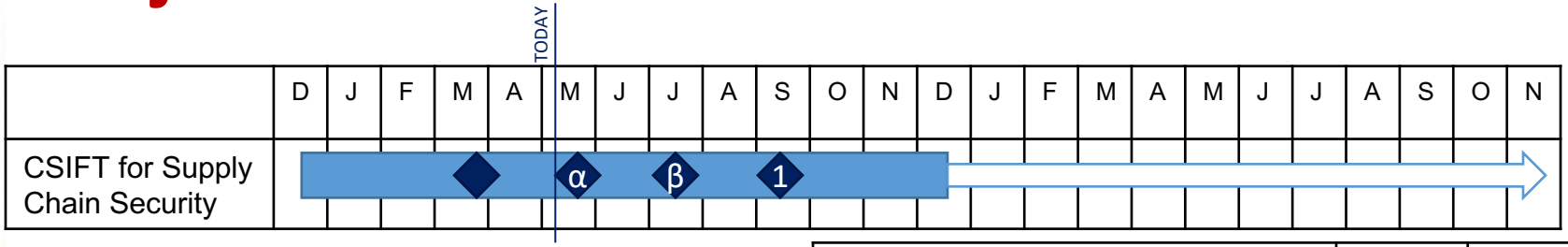
The complete solution must scale from tactical to strategic timescales, leveraging real-time data, analytic models, and domain expertise



Big Wins (so far)

- ARLIS recognition in whitepaper, and participation in follow-on working group
  - Michael Horowitz, Julia Ciocca, Lauren Kahn, Christian Ruhl. "Keeping Score: A New Approach to Geopolitical Forecasting." Perry World House, University of Pennsylvania. February 2021. https://global.upenn.edu/perryworldhouse/keeping-score-new-approach-geopolitical-forecasting
  - PRIAM (Predictive Intelligence Assessment Methods) Working Group
- Initial work on visual analytics platform for decision maker
- Whitepapers circulating at policymaker- and analyst-levels
  - Avril Haines, Stephanie O'Sullivan, and CSIS Technology and Intelligence Task Force, "Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation." Center for Strategic and International Studies (CSIS), January 2021, www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation

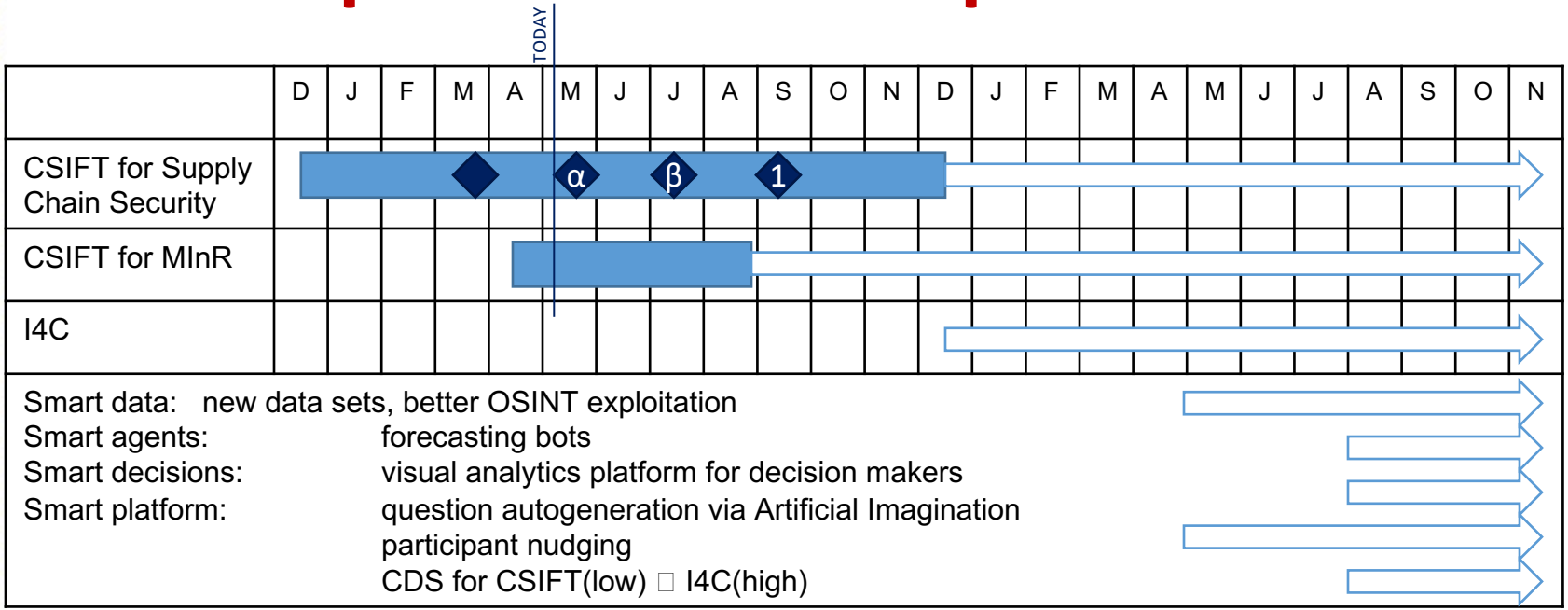
Project Status



Key Deliverables/ Insights / Activities	Timeline / status	R/Y/G
Select use case / topic area	4/1/21	COMPLETE
Define compute resources	5/1/21	COMPLETE
Roadmap and recommended business model	11/1/21	On track
Deploy tool	9/1/21	On track
Define and release initial questions	10/1/21	On track

- Alpha demo in May
- Beta launch, with launch event, July
  - Ideas for keynote speaker? Ideas for participants?
- Live launch event, September
  - Ideas for keynote speaker? Ideas for participants?
- Risk: transition, transition, transition
  - IF we launch a tool without a stakeholder THEN THERE IS A RISK THAT we are not impacting mission RESULTING IN lack of transition. Mitigation: use Alpha demo to make outreach more compelling.
  - IF we launch a tool without a crowd THEN THERE IS A RISK THAT the system will not generate data/insights RESULTING IN lack of transition. Mitigation: bootstrap crowd with professional organizations, academic contacts; foster initial forecasting with live events.
  - IF we have a successful platform in December but no follow-on funding THEN THERE IS A RISK THAT we turn off the system RESULTING IN an attention gap, and a need to restart the engine.

Next Steps and Future Capabilities



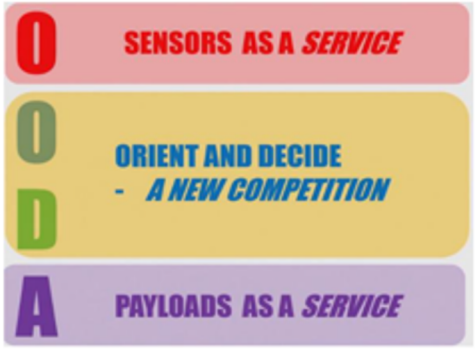
Support to A Navy Decision Science Strategy (SANDS2)

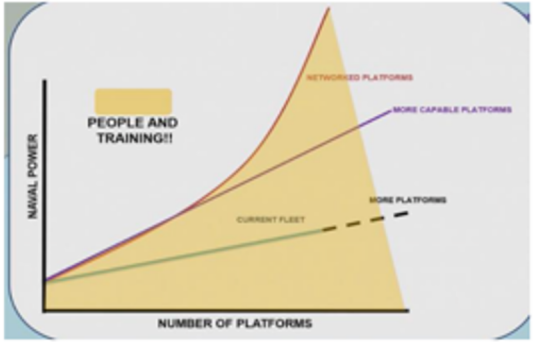
Support to A Navy Decision Science Strategy (SANDS2)

- Sponsor: Office of Naval Research
- Program Manager/Client: Dr. Peter Squire
- Period of Performance: 11/09/20 – 11/08/21
- TRL of the work: 6.1
- Total Budget (+ Expenditures to Date): $407,923.00 ($64,746)
- Team Members:
  - PIs: Adam Russell, ARLIS; Dr. Mike Dougherty, UMD/Psychology
  - ARLIS Team members: Bernadette Jerome, Susan Campbell, David Martinez, Jana Schwartz, Devin Ellis
  - UMD Team Members: Rosalind Nguyen
  - GT Team Members: Dr. Rick Thomas, Justin Sukernek, Jeremy Gibson

SANDS2 Goal:
Enable USN Decision-Advantage

- **Decision-making as the next "Revolution in Military Affairs"?**





"The game goes to the continuous thinker."

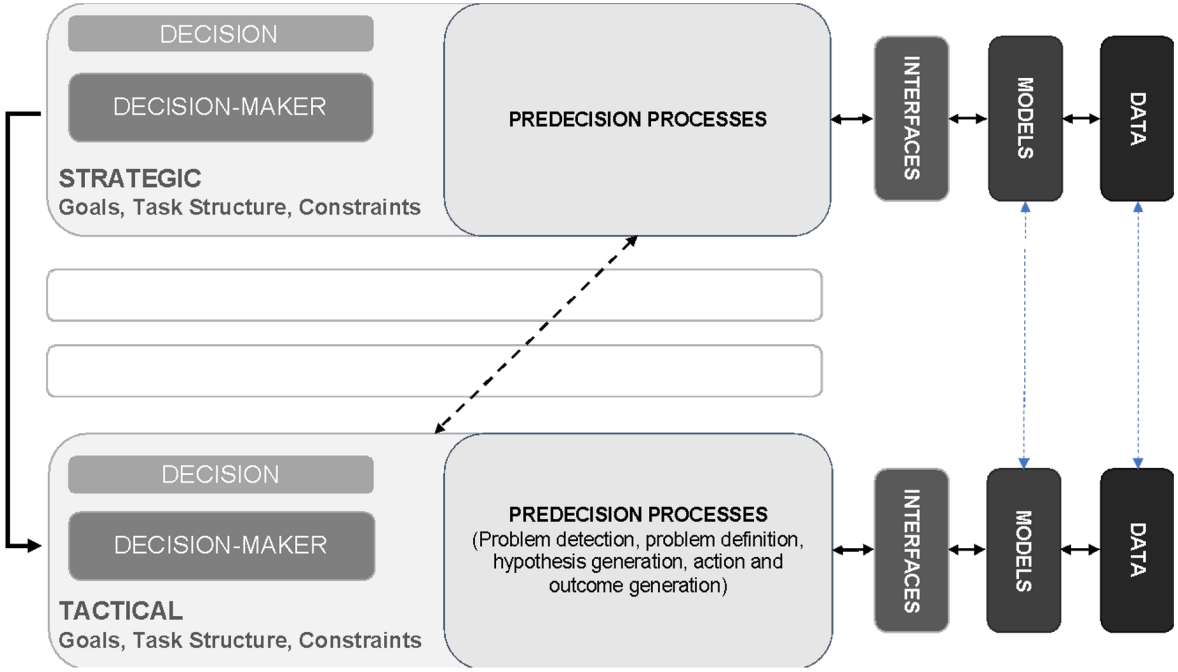
SANDS2 Overview

Goal: Help ONR use Decision Science to improve "**decision supply chains**" for advantage

Expected Impact: Inform investments in Decision Sciences and Decision Tools by creating a decision-making *lingua franca* via a Decision Science Strategy Framework (DSSF), lexicon, and R&D strategy

Success measures: transition to (and use by) ONR/USN, wargaming communities, and other decision support systems/programs/R&D

Decision Science Strategy Framework (DSSF) - Beta



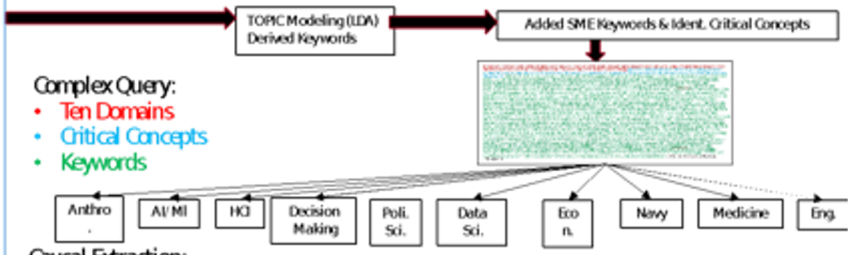
Informs:

- Lingua Franca
- Failure Mode Analyses and "Noise"
- Optimal vs Competitive
- R&D opportunities

DSSF: State of the Science & Lexicon

Decision-Making & Decision Support Systems Corpora

- Chance: Decision
- International Journal of Forecasting
- Journal of Behavioral Decision Making
- Journal of Benefit-Cost Analysis
- Journal of Behavioral Public Administration
- Journal of Economic Psychology
- Journal of Forecasting
- Journal of Multi-Criteria Decision Analysis
- Journal of Risk and Uncertainty
- Medical Decision Making
- Organizational Behavior and Human Decision Processes
- Policy Insights from the Behavioral and Brain Sciences (PBBS)
- Theory and Decision
- Thinking and Reasoning
- Cognitive Engineering and Decision Making
- Psychological Review



Causal Extraction:
- Applied to each domain corpus
- Stanford NLP Parser
- Causal Extraction via Odinson

Nomo Net:
- Causal Extractions
- Causal (Sub) Graphs
- Network Analyses (Domain Overlap, Uniqueness, Centroids, etc.)

Inform:
- Decision Framework
- Lexicon
- Navy R&D Roadmap

A Lexicon for the Decision Science Strategy Framework (DSSF)

SANDS2 Team

February 2021

1 Introduction

Decision science is an interdisciplinary field of scientific study that seeks to understand and improve judgment and decision making within individuals, groups, and populations. As part of a larger research effort to support the Office of Naval Research's interest in incorporating decision science within its research portfolio related to enhancing Navy decision-making, this document summarizes and describes key elements of the Decision Science Strategy Framework (DSSF) developed by the SANDS2 team at the University of Maryland and The Georgia Institute of Technology. The document contains a section on major constructs within the framework, as well as a list of key terms and their definitions, as derived from an analysis of the decision science literature. Although decision making can be considered a very broad construct, it is important to differentiate among decision making and other components of the decision system that may serve as input to or support for a particular decision. It is for this reason that our DSSF – and this lexicon – seek to embed decision-making and decision science within the larger context of any individual's and organization's respective "decision supply chains".

Our framework draws the distinction between problem solving and decision making. Although *overt* problem solving activities typically involve one or more decisions, not all decisions are necessarily an act of *overt* problem solving. Problem solving is often characterized as a broad activity that involves identification of an initial state, intermediate states, and goal states, as well as algorithms (i.e., operators) for moving from one position in the problem space to the next. Although decision making is required for navigating the problem space (e.g., deciding amongst courses of action, selecting amongst problem solving operators, choosing amongst plans, etc), many decisions are made without necessarily addressing a specific overt problem. Few academic researchers identify themselves as studying problem solving per se, but instead study processes that are necessarily for problem solving.

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
DRAFT: DSSF – State of the Science - Lexicon	APR 2021	Delayed
DRAFT: (Red-teamed) DSSF-informed R&D strategy	JUL 2021	On Schedule
Final Report	OCT 2021	On Schedule

- **Big Wins (so far)**: Draft DSSF has informed multiple discussions, expanded focus on ”decision supply chains.” Collaborating with CPG on Lexicon and Lit Review to maximize value to ONR
- **Transition goals/obstacles**: None to date
- **New ideas and whitepapers**: Wargaming engagement, computational models of “decision supply chains”
- **Sponsor relationship, new/additional sponsors**: ongoing

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

FY22 Internal Research & Development Projects

Mission Area Session

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Automatic Identification of Narratives

Brook Hefright, Associate Research Scientist

bhefright@arlis.umd.edu

Automatic Identification of Narratives

- Sponsor: ARLIS, this is an IRAD project
- Program Manager/Client: OUSD/I&S
- Period of Performance: 6 months, beginning May 2021 pending researcher availability
- Total Budget: $50K, expenditures to date $0
- TRL of the work: TRL 1-3, research to prove feasibility
- Team Members:
  - PI: Brook Hefright
  - Team Members: Ewa Golonka, Anton Rytting, graduate student

Project Description

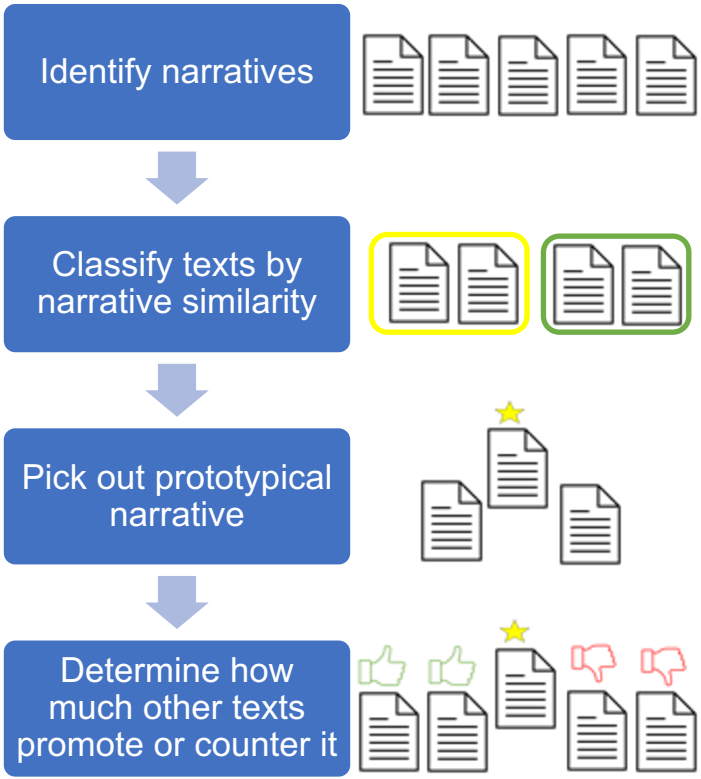
Integrates ARLIS's capabilities in social and behavioral science, AI, and computing to enable at-scale analysis of open-source intelligence and support just-in-time influence operations. Serves as a building block for ARLIS's "social weather forecasting" program.

Goal: Enable OSINT analysts to identify emerging narratives in a large collection of texts, including multilingual texts and social media, so that DOD, IC, and diplomatic actors can mount rapid response.

Expected Impact: Will enable USG to analyze and respond to narratives that impact national interests. Has applications in any field that needs to understand not just *what* people believe, but *why*: advertising, political consulting, customer service.

Success measures: Current phase: (1) demonstrate feasibility of automatic detection of "minimal narratives" in English text; (2) secure sponsor funding for further development.

Automatic Detection of Narratives



Project objective: Determine feasibility of computational techniques to identify narratives in written text.

Deliverables:

- Targeted lit. review
- Experiment design and identification of corpus
- Tech. report, whitepaper

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Targeted literature review	2 months	On schedule
Experiment design and identification of corpus	4 months	On schedule
Technical report and whitepaper	6 months	On schedule

- **Big Wins (so far)**: Project will begin May 2021 pending researcher availability.
- **Transition goals/obstacles**:
  - Goal: Develop whitepaper to find sponsor and develop capability.
  - Obstacle: USG OSINT and influence efforts are in flux.
- **New ideas and whitepapers**: Whitepaper is one of the deliverables.
- **Sponsor relationship, new/additional sponsors**: Prospective sponsors: DOD/DIA, CIA/OSE, ODNI/NMEC, NVTC, State/GEC.

Thank you!

Brook Hefright

bhefright@arlis.umd.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Identifying and Tracking Russian Operations in the Information Environment (OIE) in Central Asia

Marilyn Maines, ARLIS
mmaines@arlis.umd.edu

Barnett Koven, START
bkoven@umd.edu

Identifying and Tracking Russian Operations in the Information Environment (OIE) in Central Asia

- Sponsor: ARLIS
- Program Manager/Client: OUSD/I&S
- Period of Performance: 6 months, beginning May 2021
- Total Budget: $75k, expenditures to date: $0
- TRL of the work: TRL 2-3, research to prove feasibility
- Team Members: Joint ARLIS-START project
  - Co-PIs: Marilyn Maines and Barnett Koven
  - ARLIS: Brook Hefright, Ewa Golonka, Anton Rytting, Victor Frank
  - START: Steve Sin, Devin Ellis, Katy Lindquist, Rhyner Washburn, Madeline Romm

Project Description

- ARLIS and START will combine efforts for a two-part research effort focused on identifying and tracking Russian OIE in Central Asia related to economic development projects in the region.
- Part 1: START will identify characteristics and techniques used in OIE by Russia at the strategic and operational levels.
- Part 2: ARLIS will identify and track the prevalence of narratives (stories, messages, or message elements) related to recent Russian economic projects in Central Asia.
- This research will also focus attention on Russian OIE efforts aimed at discrediting the U.S. and/or limiting U.S. influence in the region.

Project Description

Relation to ARLIS story:

OIE is one of the key research areas within the Cognitive Security core research mission.

This project will provide:

1) understanding of Russian OIE techniques and practices in Central Asia

2) reusable narrative content for future research efforts and simulations in the Cognitive Security Proving Ground

3) will also complement ARLIS research already conducted on Chinese Belt and Road (BRI) economic development efforts in Africa.

4) Will connect with other narrative work – Minerva project on analyzing social media narratives, IRAD project on automatic identification.

Project Description

Goal:
This work will enable the USG to understand the intentions and breadth of Russian information operations in a neighboring geographic region that is also of high interest to China and the U.S.

Expected Impact:
This project will provide information that has the potential to better prepare the USG to recognize and resist Russian OIE efforts and techniques currently used against the United States and its allies and partners.

Success measures:
1) When ARLIS' approach to narrative identification is recognized by other experts in the field.
2) When START's analysis of Russian OIE characteristics and techniques is cited by other experts.

Identifying and Tracking Russian Operations in the OIE in Central Asia: Project Overview

Project objectives:

Part 1: (START) Determine how OIE fits into the larger strategic maneuvers for Russia as well as the desired effects sought from OIE efforts in Central Asia.

Part 2: (ARLIS) Identify and track the prevalence of narratives (stories, messages, or message elements) related to recent Russian OIE efforts in Central Asia.

Deliverables:

1.1. Analysis of Russian 'doctrinal' thinking on OIE.
1.2. Assessment of Russian efforts OIE in Central Asia.
1.3. Comparison of actual Russian OIE efforts with 'doctrinal' thinking.
2.1. Corpus of texts that contain narratives designed to impact foreign perceptions of Russian economic projects in Central Asia.
2.2. Technical report documenting narrative development, introduction, and propagation.

Project Status and Next Steps

Key Deliverables/ Insights / Activities	Timeline/ status	R/Y/G
Analysis of Russian doctrinal thinking on OIE compared with actual OIE practices in Central Asia	6 months	On schedule
Collection of narratives (stories, messages, message elements) focused on Russian economic activity in Central Asia (reusable by CSPG)	6 months	On schedule
Additional focus on Russian efforts to discredit the U.S. or limit U.S. influence in the region.	6 months	On schedule

- **Big wins (so far)**: Project begins May 2021, hope to make a difference.
- **Transition goals/obstacles**: Create usable scenario set for CSPG.
- **New ideas and whitepapers**: Whitepaper exists for follow-on study on Chinese OIE in the Central Asia region.
- **Sponsor relationship, new/additional sponsors**: Develop partnership with State/SCA which has USG lead "to resist Russian OIE efforts and techniques."

Thank you!

Presenters:
Marilyn Maines
mmaines@arlis.umd.edu

Barnett Koven
bkoven@umd.edu

Applied Research Laboratory for Intelligence and Security

National Consortium for the Study of Terrorism and Responses to Terrorism

University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

Programs

Session

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Intelligence & Security University Research Enterprise (INSURE)

ARLIS-led Academic Consortium

Erin Fitzgerald, ARLIS DD and INSURE Managing Director
insure@arlis.umd.edu

INSURE Consortium Overview

ARLIS as <u>the center</u> of Defense Security/IC research engagement with academia

INSURE projects:

- Must be within scope of ARLIS core competencies and of UARC character
- Must include an ARLIS lead to track progress, connect relevant stakeholders, and integrate the effort into the corresponding ARLIS portfolio

Partners admitted to INSURE based on:

- Institutional strengths
- Track record conducting applied, quick-turn, mission-relevant (and restricted?) R&D
- Capabilities for training the current workforce and growing the workforce of the future
- Institutional leadership engagement and buy-in

Pathways to funding:

1. Member engages potential sponsor directly about work and develops programming
2. Members conduct joint program development, leveraging interinstitutional strengths
3. USG agency requests R&D effort needing ARLIS partners' strengths

2021 INSURE Consortium Membership

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Current Activities

- Economic Statecraft Program, led by TAMU Bush School and funded by USAF CDM
- Human-Machine Ecosystem Laboratory, led by TAMU System and funded by NSA
- Expanding Applications for AI Automation and Augmentation including Insider Risk work led by UMD START and imagery analysis algorithms led by TAMU, funded by USAF CDM
- Five pilot projects funded by DDR&E HBCU Program Office
  1. 5G Technology Assessment -- Morgan State and Howard
  2. Machine Learning Experimentation – UDC
  3. Cyber-Assessment of AI/ML Tools -- Howard and Morgan State
  4. AI/ML Systems Engineering Workbench – Howard and Morgan State
  5. ChatBot Testbed – Howard, Morgan State, and UDC
- INSURE Value Proposition
  - Participation in the role as trusted performer for the USG
  - Academic alignment and growth to support the core competencies
  - Expansion of use-inspired and applied research opportunities
  - Regular interaction with S&T leadership of IC agencies

Directly tied to ARLIS mission activities & sponsors

"no matter who you are, most of the smartest people work for someone else."
-- [Bill] Joy's Law

Planning INSURE Activities

- Consortium Management
  - Facilitate **member coordination and research cooperation**
  - Streamline and optimize **proposal and subcontract processes**
  - Create processes to ensure **compliance** with contract security reqmts + Organiztnl COI
  - Enable **data storage, virtualization, and compute infrastructure** for restricted research
  - Inventory shareable facilities, testbeds, capabilities accessible to the DoD/IC
  - Organize a **2021 INSURE "Security Research Day on the Hill"** for legislators/staff
- Consortium Activities
  - Facilitate **collective program development** across the member institutions
  - Organize **Technical Exchange** events (with concrete follow up) with USG agencies across all INSURE/ARLIS Mission Areas
  - Organize a **network of subject matter experts** for S&T issues needing SMEs in key areas of need to OUSD(IS), DoD/IC
  - Develop curricula for **DoD/IC workforce and pipeline** training, courses, and certificates.

For more information, contact:

Erin Fitzgerald
Managing Director, INSURE
Deputy Director, ARLIS
erinf@umd.edu
insure@arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Technology and Law Academy: Training and Education Programming through ARLIS

Harvey Rishikof

rishikof@umd.edu

Concept of Operations

- Design and carry out accredited courses leading to a planned certificate and master's level degree program in Technology, Law, and National Security.
- Target audience: Senior IC and DSE Lawyers and policy practitioners
- Instructors drawn from ARLIS and broad technology and law communities
- Leverage university infrastructure, UARC mission, classified infrastructure

Activities to Date

- I&S support enabled Summer 2020 6-week pilot course on *Emerging Topics in Technology in Law*, held online due to COVID-19, and
- Spring 2021: first-of-its-kind acquisition course – *Acquiring Emerging Technologies (AET)* – focused on mid-career to senior acquisitions professionals, technologists, and other professionals across the DISE looking to solve complex problems involving acquisition of emerging technologies
  - Virtual setting culminating in a classified final exercise.

Big Win

- Curricula (with detailed reading list and assignments) developed for first two courses, and 3rd course curriculum in progress.
- Sixty attorneys from across the IC received instruction on the legal aspects of several critical technology topics in national security – 30 in a survey course across tech areas and 30 in a course tied to defense acquisition of new technologies.
- Growing interest from defense and intel communities, along with communicated willingness to pay tuition and make program self-funding

Next Steps and Future Capabilities

- Planned in-residence, classified course offering of the *Emerging Issues in Technology (EITL)* in fall 2021

Thank you!

Harvey Rishikof

rishikof@umd.edu





APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

Research for Intelligence & Security Challenges (RISC) Internship Program

Erin Fitzgerald
efitzgerald@arlis.umd.edu, risc@arlis.umd.edu

Research for Intelligence and Security Challenges (RISC)

- **Sponsors:** NGA, OUSD(I&S), ODNI
- **Program Managers:**
  Veda Bharath / Amanda McGlone / John Beieler
- **Key Dates:** 1 June – 6 August (Internship); 1Sept – 31May (follow-on)
- **Team Members**:
  - Erin Fitzgerald
  - Victor Frank
  - David Lovell
  - Sharon Beermann-Curtin
  - Rick Phillips

AIRICC 2020 Program Overview

- 10 weeks: June 1 – August 7
- Six teams of three interns working on AI problems of interest to the Intelligence Community
- 27 applicants, mostly UMD undergraduate + graduate students
- One principal faculty mentor per team
- One dedicated IC mentor engaged throughout the summer
- Regular engagement with IC subject matter experts
- Graduate research assistant as primary interface and support
- Designed as an in-person program but shifted to online model

RISC 2021 Program Overview

- 10 weeks: June 1 – August 7
- **Sixteen** teams of 2–3 interns **(40 total!)** working on problems of interest to the **Defense Security & Intelligence Communities**
- **105** applicants **from 15 universities** (undergrad + grads)
- One principal faculty mentor per team
- One dedicated USG mentor engaged throughout the summer
- Regular engagement with USG subject matter experts
- Graduate research assistant as primary interface and support
- Designed as an **online program**

Goals for RISC

- 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 DISE and IC's future technical workforce
- **Support talented students and important projects into academic year + initiate security clearances**

RISC 2021 Interns

- Forty interns selected from 105 candidates
- From: Citadel, Drexel, GMU, GWU, GT, Howard (HBCU), JMU, JHU, TAMU, UMD, U Wisconsin, Yale
- 14 undergraduates, two MS students, one PhD student
- Technical disciplines include:
  - Computer Science
  - Computer Science & Biological Sciences
  - Computer Engineering
  - Mechanical Engineering
  - Aerospace Engineering
- Wide variation in experience with ML/AI and research broadly
- A few interns with some exposure to national security research

RISC 2021 Project Topics

- A: Improving Solid 3D Modeling From Point Clouds
- B: Algorithms for Anomaly and Threat Detection

NGA

- C: Open-source research to support permafrost mapping
- D: Declassification System Modernization Project
- E: Security Enterprise Oversight Metrics
- F: Evaluating and Optimizing Security Training

DISE

- G: C2IE Strategic Messaging Effects
- H: Assessment of Threat/Opportunity space for IC involvement/usage of public open-source projects
- J: Securing Critical Infrastructure
- K: CircleFinder on Google Cloud

ODNI

- M: A2E2 (DARPA)
- N: Social Media Simulator for Cognitive Security (I&S)
- O: Insider TRUST (I&S)

Augmenting ARLIS

- P: Augmented Collective Intelligence for Insider Threat Forecasting (I&S)
- Q: Adversary Perceptions of U.S. Performance against COVID-19 pandemic (HHS)

Engage with the RISC program!

- June 1 kickoff
- Give a Lunch ‘n’ Learn Seminar
- August 4: Final Presentations
- Consider supporting students for follow-on work!

Email risc@arlis.umd.edu to learn more.


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY
UNIVERSITY OF MARYLAND

Questions?