THE UNIVERSITY OF ARIZONA

INTELLIGENCE OPERATIONS

# DEAD DROP

INTELLIGENCE | PEOPLE | IDEAS | IMPACT

## INTELLIGENCE IN THE AGE OF AI

The future of intelligence and information operations

## GLOBAL TRENDS SHAPING TOMORROW

Emerging issues influencing intelligence and security

## STUDENT SUCCESS & OPPORTUNITIES

Courses, upcoming events and resources

FALL 2026

COLLEGE OF ENGINEERING

Intelligence Operations

# IN THIS ISSUE


**03** **From the Classroom to the Contemporary Security Environment**
Why Intelligence and Information Operations Matter

**09** **Global Trends Shaping Tomorrow**
Real-World Perspectives

**11** **Fall 2026 Course Schedule**
15 Week, 7 Week 1st, and 7 Week 2nd

**14** **Advising Corner**
Guidance, Resources, Support

**15** **Events & News**
Speaker Series, Opportunities


*"Intelligence is not just a profession, it’s a perspective."*



# From the Classroom to the Contemporary Security Environment

## Why Intelligence and Information Operations Matter More Than Ever

**By Craig Nazareth, Associate Professor of Practice**

The Intelligence and Information Operations program at the University of Arizona College of Engineering allows students to examine security problems in a collaborative academic environment across the core and elective framework within the program. Intelligence problems rarely fit within a single discipline. Understanding them requires examining the interplay between intelligence disciplines, emerging technologies, human behavior and decision-making, and the increasingly complex information environment in which competition and conflict occur. Current conflicts provide a powerful lens through which to make these connections, while demonstrating how the knowledge and competencies developed across the IIO program translate to the problems our graduates may encounter in the workforce.

The U.S.-Israeli-Iran conflict brings students face to face with a complex strategic problem spanning nearly every dimension of intelligence and information operations. Examining Iran's nuclear ambitions, regional influence, ballistic missile capabilities, and proxy forces illustrates how intelligence supports efforts to understand adversary capabilities and intentions while competing actors wield information as an instrument of power. The conflict also highlights the challenge in establishing ground truth from competing narratives that have shaped policy and public perception.

Operation Midnight Hammer provides a compelling example of how intelligence, military operations, and strategic communication intersect, while illustrating the difficulty of establishing ground truth following military action. On June 21st and 22nd 2025, U.S. B-2 stealth bombers penetrated contested airspace in Iran to strike underground nuclear



facilities at Fordow and Natanz while tomahawk missiles struck Esfahan’s nuclear facilities as part of a coordinated operation following the initiation of Israeli military strikes against Iran earlier that month (U.S. Department of War, 2025). During the Israeli and U.S. strikes, U.S. and Israeli intelligence agencies likely monitored Iranian integrated air and missile systems, including radar emissions and communications, and other indicators that could reveal a threat to the strike package. Following the strikes, ground, space-based, and airborne sensors were likely used to assess the physical and functional impacts on Iran’s nuclear development program, and whether operational objectives were achieved.

Intelligence agencies also likely weighed classified assessments against all other available information and intelligence, including public reporting. Director of United Nation’s International Atomic Energy Agency reported on June 20th that Israel had struck the Natanz enrichment site, and “…destroyed electrical infrastructure at the facility…[and]… functionally destroyed the Pilot Fuel Enrichment Plant” (IAEA, 2025). Israeli strikes had also damaged uranium conversion and enrichment infrastructure, but the Director stated that there was no apparent damage at Fordow, or Iran’s nuclear power plants at Tehran and Bushehr (IAEA, 2025). Based on Operation Midnight Hammer’s timing and targets, it is apparent that intelligence agencies not only amassed precise targeting information using various intelligence disciplines to collect sensitive data on the sites and determine the situation following the Israeli strikes, but the U.S. had been designing and integrating weapons into bombing tactics to precisely and effectively target deep buried nuclear facilities in Iran, capabilities the Israel forces may not have had.

According to Department of Defense reporting, the design of the weapons and operational plans for




striking Iran's deeply buried nuclear facilities had been under development for approximately 15 years (Lopez, 2025). President Donald Trump and Secretary of War Pete Hegseth publicly emphasized the success of the operation and U.S. military capabilities, while news organizations, independent analysts, and online observers examined commercially available imagery and other information to offer their own assessments. What could be established was that Iranian nuclear facilities at Natanz and Esfahan were struck due to their roles in uranium enrichment and related nuclear activities, while the U.S. also employed 30,000-pound GBU-57 massive ordnance penetrator bombs against the deeply buried Fordow Fuel Enrichment Plant (FFEP), near Qom, Iran (Lopez, 2025). The strikes resulted in observable damage to the facilities, although uncertainty remained regarding their effects on Iran's broader nuclear development capability (Murphy & Irish, 2025).

In February 2026, the United States initiated further military operations against Iran, pursuing objectives that included degrading Iran's ballistic

missile capabilities, naval forces, defense industrial infrastructure, and potential pathways to nuclear weapons. These developments raise important questions about the relationship between tactical and operational success and the achievement of broader strategic objectives. While the White House has emphasized the effectiveness of U.S. military operations, analysts have examined whether battlefield achievements necessarily translate into enduring strategic advantages. Daniel Byman (2026), an analyst at the Center for Strategic and International Studies, argues that wars are determined by more than battlefield performance and that Iran may achieve strategic advantages through its ability to endure military pressure, impose costs, and shift the conflict's consequences beyond the battlefield. His assessment illustrates how competing interpretations of military effectiveness and strategic outcomes can shape the information environment, public perceptions, and subsequent policy decisions. For IIO students, these competing assessments illustrate why establishing ground truth requires distinguishing observable military effects, intelligence assessments, strategic objectives, and the narratives through which governments and other actors communicate their interpretation of events.




However, if Operation Midnight Hammer illustrates how intelligence, military operations and information intersect during a highly coordinated strategic operation, the Russia-Ukraine war illustrates these same principles across the domains of warfare with specific focus at the tactical level. The Russia-Ukraine war provides IIO students a novel lens through which to appreciate how quickly military technologies and tactics adapt under operational pressure, and the resulting implications for intelligence and information operations. The war has featured significant developments in autonomous systems, cyber and electronic warfare, and information operations, and a unique view into the increasingly sophisticated integration of sensors and lethal capabilities across tactical lines and in deep areas within Russia and Ukraine (Slusher, 2025). Perhaps no technology has had a more visible impact on military strategy and tactics than the mass deployment of dual-use drones, providing first person sensing and lethality in a highly mobile, low-profile, and relatively inexpensive package.

Across the nearly 1,600-kilometer front lines in Ukraine, including “…Russia-occupied territories in eastern and southern Ukraine” (U.S. Department of State, 2024), small First Person View (FPV) “… surveillance and attack drones…” (Reuters, 2026) mercilessly hunt the landscape to detect, discriminate, and strike military targets (LiveUAmap.com, n.d.; Reuters, 2026). This form of drone warfare has dramatically impacted unit strategy and tactics, reducing military formations of armored and infantry units to lone warriors struggling to survive for months in remote foxholes and outposts. Columns of Russian tanks and armored personnel carriers that began the war in formation became easy targets for cheap drones as the war progressed, now in its fourth



year. Thus, the conflict has been reduced to very small unit maneuvers involving individuals, not large formations, and increasingly integrated lethal and non-lethal drones enabling cyber and electronic capability employment in an ongoing contest to gain small strips of land and create salients for ongoing pressure along the front lines.

IIO students confront these issues throughout the curriculum, studying radio frequency (RF) propagation and signals, signals intelligence (SIGINT) and electronic warfare (EW), and open-source intelligence. Students can ask how Ukrainian and Russian SIGINT and EW systems detect, locate, exploit, and disrupt drone control and navigation signals, They can also examine how countermeasures offset tactical or operational advantages in time and space such as drone operators changing frequencies or tactics, or Russian or Ukrainian forces employing physical fiber optic command lines to control the drones without relying on vulnerable radio frequency control links. These case studies also provide a unique perspective into information collection and the case for computational and engineered solutions to solve hard collection and processing problems. Thus, the integration of artificial intelligence (AI) and other advanced sensing approaches (classical versus quantum) adds another dimension to this problem: how can increasingly large volumes of information be processed, exploited, and disseminated to support effective intelligence analysis and collection, lethal and non-lethal targeting, and decision-making?

Another equally important question confronts us. How can advanced sensing approaches detect low probability of intercept and low probability of detection signals, or sift through faint signals among the noise and fog of competition in gray-zone competition and war?

Whether supporting operations in Iran or Ukraine, monitoring strategic competition, or addressing emerging threats elsewhere, analysts confront a continuous flow of data from on-ground human reporting, technical sensors, open sources, online content curators and increasingly sophisticated digital personas. The volume, variety, and uncertain sourcing of this information increasingly challenges notions of “trusted” sources and creates demand for authenticated data that can be distinguished from incomplete, deceptive, or intentionally obscured information. The need for more effective automation to take on traditionally human tasks with effective guardrails to support various intelligence functions and targeting processes also becomes glaringly evident. AI provides new methods to help analysts process the sheer volume and variety of signatures, signals, imagery, text and other data, identify relationships and anomalies, and focus human attention on information most relevant to the intelligence problem. AI also aids in managing thousands of technical sensing capabilities while processing, exploiting, and disseminating information and intelligence to decision-makers and early warning systems.

The previously mentioned case studies demonstrate why intelligence problems cannot be understood through a single discipline or solely by humans. A deeply buried nuclear facility in Iran is simultaneously a collection, sensing, analysis, targeting, and information problem. A low-cost FPV drone operating along the front lines in Ukraine presents questions involving RF propagation, SIGINT and EW, sensing, targeting, ISR synchronization, and increasingly, AI. Understanding either problem requires students to connect what they learn across the IIO curriculum rather than view individual courses as isolated subjects.

This is where the interdisciplinary structure of the IIO program becomes particularly relevant. Courses in intelligence analysis and collection establish how requirements are developed, information is evaluated, and uncertainty is communicated. Signals intelligence, advanced sensing, and ISR synchronization examine how sensors can find and fix difficult targets and signatures across time and space. Target-centric analysis and intelligence support to targeting help students understand systems, relationships, vulnerabilities, and desired goals with respect to the target. Information warfare and open-source intelligence expose students to an environment where adversaries, governments, media organizations, online communities, and increasingly sophisticated digital personas compete to shape what people see, believe, and understand. AI adds another layer, providing computational approaches for managing sensors, processing information, identifying patterns, and helping humans make sense of increasingly complex intelligence problems.

The enduring value proposition for IIO students is that they gain the ability to recognize an intelligence problem, ask the right questions, determine what information is needed, evaluate what can be trusted, connect information across disciplines, and communicate what is known, what is assessed, and what remains uncertain. This is where the classroom meets the contemporary security environment. The concepts encountered across the curriculum are already playing out in the conflicts, technologies, intelligence challenges, and information environments examined daily. The objective is not simply to comprehend what is happening today, but to develop the interdisciplinary knowledge and skills to understand, anticipate, and contribute to solving the intelligence and information problems of tomorrow.



References

Byman, D. (2026, April 2). Who is winning the Iran war? Center for Strategic and International Studies. https://www.csis.org/analysis/who-winning-iran-war

International Atomic Energy Agency. (n.d.). Overview of management, governance and organizational structure.https://www.iaea.org/about

International Atomic Energy Agency. (2025, June 20). IAEA Director General Grossi's statement to UNSC on situation in Iran. https://www.iaea.org/newscenter/statements/iaea-director-general-grossis-statement-to-unsc-on-situation-in-iran-20-june-2025

Liveuamap. (n.d.). Ukraine interactive map: Ukraine latest news on live map [Interactive map]. Retrieved October 12, 2026, from https://ukraine.liveuamap.com/en

Lopez, C. T. (2025, June 26). 'Historically successful' strike on Iranian nuclear site was 15 years in the making. U.S. Department of Defense. https://www.war.gov/News/News-Stories/Article/Article/4227082/historically-successful-strike-on-iranian-nuclear-site-was-15-years-in-the-maki/

Murphy, F., & Irish, J. (2025, June 29). U.S. strikes on Iran's nuclear sites set up "cat-and-mouse" hunt for missing uranium. Reuters. https://www.reuters.com/world/europe/us-strikes-irans-nuclear-sites-set-up-cat-and-mouse-hunt-missing-uranium-2025-06-29/

Rodgers, J. (2025, June 23). What Operation Midnight Hammer means for the future of Iran's nuclear ambitions. Center for Strategic and International Studies. https://www.csis.org/analysis/what-operation-midnight-hammer-means-future-irans-nuclear-ambitions

Slusher, M. N. (2025, May 2). Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience. Center for Strategic and International Studies. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience

Zafra, M., Collett-White, M., Balmforth, T., & Hunder, M. (2026, July 23). Inside Ukraine's kill zone. Reuters. https://www.reuters.com/graphics/UKRAINE-CRISIS/KILL-ZONE/znpnojmknvl/

# GLOBAL TRENDS SHAPING TOMORROW

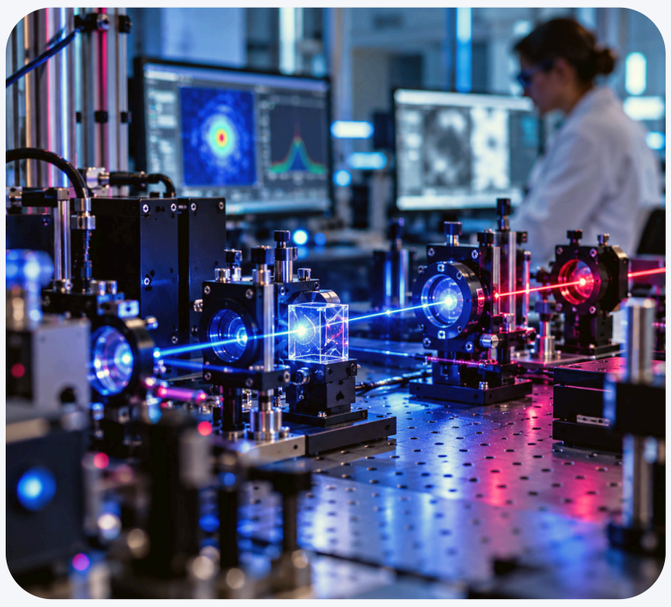
## KEY DEVELOPMENTS TO WATCH




### The AI Revolution in Intelligence

Artificial intelligence is reshaping how the U.S. Intelligence Community collects, processes, and analyzes information. From identifying patterns in massive datasets to accelerating intelligence assessments, AI offers new opportunities to improve speed and efficiency. Yet these capabilities also introduce challenges involving accuracy, transparency, and human oversight. As intelligence agencies integrate AI into their operations, the ability to combine advanced technology with experienced analytical judgment will remain essential to producing reliable intelligence.

**Further Reading:** *The Role of Artificial Intelligence in the U.S. Intelligence Community — Aspen Institute, October 2024.*



### Beyond the Visible: Quantum Sensing

Quantum sensing is emerging as a promising technology for intelligence, surveillance, and reconnaissance (ISR). By exploiting the properties of quantum physics, advanced sensors could detect subtle changes in magnetic fields, gravity, and electromagnetic signals with exceptional precision. A 2026 Defense Innovation Unit initiative seeks to accelerate these technologies for military applications, including operations in environments where conventional sensors face limitations. As development progresses, quantum sensing could expand how intelligence professionals detect, monitor, and understand activity across complex operational environments.

**Further Reading:** Quantum Sensing Explained — NIST; Department of War Announces Initiative to Revolutionize ISR via Quantum Sensing — June 2026.



### The Next Technology Race

Technological innovation is becoming an increasingly important factor in national security and strategic competition. The Department of War has identified six Critical Technology Areas, including applied artificial intelligence, quantum technologies, hypersonics, and directed energy, to guide defense research and investment. Many of these advancements have potential applications across both civilian and military sectors. As nations compete to develop and deploy emerging capabilities, understanding the relationship between technological progress, intelligence operations, and national security priorities will become increasingly important.

**Further Reading:** *Critical Technology Areas — Department of War, Office of the Under Secretary for Research and Engineering; Senior Officials Announced for Six Critical Technology Areas — January 2026.*

# GLOBAL TRENDS SHAPING TOMORROW

## KEY DEVELOPMENTS TO WATCH




### AI in Modern Policing

Artificial intelligence is transforming law enforcement by helping agencies identify crime trends, analyze large datasets, and allocate resources more effectively. From intelligence analysis and digital evidence review to administrative efficiency, AI offers new opportunities for agencies of all sizes. However, successful adoption requires careful testing, human oversight, and clear ethical guidelines. As these technologies become more accessible, understanding their capabilities and limitations will be increasingly important for future law enforcement and intelligence professionals.

**Further Reading:** *AI in Policing Beyond the Early Adopters: What Your Agency Can and Should Do — National Policing Institute, April 2026*



### China-Taiwan: The 2027 Question

Growing tensions between China and Taiwan are raising important questions about regional security and future military developments. Analysts point to 2027 as a potential turning point, citing China's military modernization, political objectives, Taiwan's upcoming elections, and shifting strategic advantages. While conflict is not inevitable, these converging factors highlight the importance of examining state interests, strategic motivations, and warning indicators. Understanding these dynamics provides intelligence professionals with a valuable framework for anticipatory analysis and assessing potential geopolitical developments.

**Further Reading:** The Dragon and the Clock—2027 as the Turning Point Year Between China and Taiwan — Institute for National Security Studies, January 2026

# SPRING 2027 COURSE SCHEDULE

**Regular Academic Session**

| COURSE # | COURSE TITLE | PROFESSOR |
|---|---|---|
| **INTV 322** Main Campus | Intelligence: Historical, Ethical, & Legal Foundations | Gary Packard |
| **INTV 326** Main Campus | Introductory Methods of Intelligence Analysis | Emilio Arias |
| **INTV 330** Main Campus | Applied Single Agent AI for Intelligence Operations | Jacob Denno |
| **INTV 330** | Applied Single Agent AI for Intelligence Operations | Jacob Denno |
| **INTV 430** | Applied Multi Agent AI for Intelligence Operations | Jacob Denno |
| **INTV 459** Main Campus | Intelligence, Surveillance & Reconnaissance Synchronization | Emilio Arias |
| **INTV 498** | Senior Capstone in Intelligence & Information Operations | Joshua Santos |
| **INTV 498** | Senior Capstone in Intelligence & Information Operations | Craig Nazareth |

# SPRING 2027 COURSE SCHEDULE

## Seven Week - First

| COURSE # | COURSE TITLE | PROFESSOR |
|---|---|---|
| **INTV 230** | Modulation & Keying | Sean Dougherty |
| **INTV 305** | Introduction to Intelligence & Information Operations | Jared Melillo |
| **INTV 322** | Intelligence: Historical, Ethical, & Legal Foundations | Mary Beth Melchior |
| **INTV 322** | Intelligence: Historical, Ethical, & Legal Foundations | Patrick Tortorici |
| **INTV 326** | Introductory Methods of Intelligence Analysis | Lachlan Galbraith |
| **INTV 326** | Introductory Methods of Intelligence Analysis | Michael Baucum |
| **INTV 351** | Signals Intelligence and Electronic Warfare | Ashley Hurst |
| **INTV 353** | Geospatial Intelligence | Billy Zsambok |
| **INTV 354** | Principles of Open Source Intelligence | Cynthia Hetherington |
| **INTV 354** | Principles of Open Source Intelligence | John McCary |
| **INTV 437** | Deception, Counter-Deception & Counter-Intelligence | Paul Cromwell |
| **INTV 450** | Information Warfare | Joseph Giordano |
| **INTV 455** | Target-Centric Analysis | Blake Empey |
| **INTV 458** | Advanced Sensing | Craig Nazareth |
| **INTV 459** | Intelligence, Surveillance & Reconnaissance Synchronization | Tyler Wisecup |

*Note: Course offerings are subject to change. Please refer to the official University of Arizona class schedule for the most current information.*

# SPRING 2027 COURSE SCHEDULE

## Seven Week - Second

| COURSE # | COURSE TITLE | PROFESSOR |
|---|---|---|
| **INTV 240** | Principles of SIGINT & EW | Sean Dougherty |
| **INTV 322** | Intelligence: Historical, Ethical, & Legal Foundations | Patrick Tortorici |
| **INTV 322** | Intelligence: Historical, Ethical, & Legal Foundations | Mary Beth Melchior |
| **INTV 326** | Introductory Methods of Intelligence Analysis | Paul Pineda |
| **INTV 326** | Introductory Methods of Intelligence Analysis | Michael Baucum |
| **INTV 350** | Intelligence Collection | Manuel Felix |
| **INTV 354** | Principles of Open Source Intelligence | John McCary |
| **INTV 354** | Principles of Open Source Intelligence | Melissa Newberg |
| **INTV 377** | Psychological Operations | Paul Cromwell |
| **INTV 427** | Intelligence Support to Targeting | Craig Nazareth |
| **INTV 450** | Information Warfare | Joseph Giordano |
| **INTV 459** | Intelligence, Surveillance & Reconnaissance Synchronization | Emilio Arias |
| **INTV 459** | Intelligence, Surveillance & Reconnaissance Synchronization | Tyler Wisecup |
| **INTV 496** | Special Topics in Intelligence & Information Operations | Patrick Tortorici |

*Note: Course offerings are subject to change. Please refer to the official University of Arizona class schedule for the most current information.*

# ADVISING CORNER

## GUIDANCE. RESOURCES. SUPPORT



**PAMELA SCANLON**

**GABRIELA SIQUEIROS-PORRAS**



### A Message from your Academic Advisors:

- Reaching out to your instructors early is recommended if you have questions about your assignments or class material. Utilize faculty office hours when needed.
- If you have hit a speed-bump, let your advisor know. We are here to problem-solve.
- How to Schedule an Advising Appointment:
  1. Sign-in to Trellis Advise using your NetID and password.
  2. Click on the link "Meet with my Advisor" under your advisor's picture - you can view all Appointments and Virtual Drop-In Sessions available.
- The THINK TANK academic support center provides free tutoring support, academic coaching (4 free sessions per semester), writing feedback and more.
- Center for Career Readiness (CCR) workshops and events, visit career.arizona.edu
- Check out Drop-In Coaching at LifeLab: Meet one-on-one with a Career Educator or Internship Coach for 10-20 minutes for a quick resume or cover letter review or to ask questions about your internship or job search. Monday – Friday, 12pm to 5pm, LifeLab. (Zoom, In-Person and via Email)

**YOUR PATH. YOUR GOALS.**
**WE'RE HERE TO HELP**

EVENTS & NEWS

# UPCOMING EVENTS & OPPORTUNITIES

CONNECT | LEARN | GET INVOLVED

**NOV 17**

## IC Speaker Series

Beyond Traditional Intelligence:
Exploring Alternative Career Paths

4:00 PM (AZ) | Virtual

**NOV 26-27**

## Thanksgiving Break

**DEC 11-17**

## Finals Week

**DEC 18**

## Winter Convocation

2:00 PM | Centennial Hall

**JAN 13**

## Spring Semester Begins



COLLEGE OF ENGINEERING
Intelligence Operations

# Student Worker

Join our team and support real world government training development!

## Details

Gain real world experience and make a difference in the readiness of Intelligence Professionals.

As a member of our scenario development team, you will learn to leverage the most recent AI tools to create hyper-realistic scenario data that represents the complexity of the real world. You will learn how to develop virtual persona actions and establish patterns of life that will be used y real Intelligence professionals to train on critical Intelligence functions.

## REQUIREMENTS:

- Remote position
- $15.15 per hour
- Max of 20 hours per week
- Enrolled in a minimum of 6 units



**PLEASE SEND YOUR RESUME AND ANY QUESTIONS TO:**

Carla Buldrini
cbuldrini@arizona.edu

Intelligence Community Centers for Academic Excellence
*Diversity. Knowledge. Excellence.*

Cyber Convergence Center

COLLEGE OF ENGINEERING
Intelligence Operations

# IC Speaker Series

# Beyond Traditional Intelligence: Exploring Alternative Career Paths

## When

November 17th
4PM AZ Time

## Where

Virtual Session - Zoom

## Guest Speakers



Melissa Newberg



Jared Melillo



Emma Murray



Lachlan Galbraith

Register Here

Intelligence Community Centers for Academic Excellence
*Diversity. Knowledge. Excellence.*

Cyber Convergence Center

# About the Speakers

## Melissa Newberg



Melissa Newberg is the Global Head of Intelligence at Seerist, where she leadsthe company's intelligence strategy and oversees a globally distributed team delivering real-time risk intelligence and strategic geopolitical analysis.

She brings more than 15 years of experience across government and the private sector. Prior to joining Seerist, Melissa spent nearly six years at Meta, where she led the Global Protective Intelligence team, and a decade as a U.S. Air Force civilian intelligence professional, serving in roles at the Pentagon and in Europe. She also served as a Department of Defense Legislative Fellow in the U.S. House of Representatives.

Melissa holds a master's degree in Near and Middle Eastern Studies from the University of Manchester and a bachelor's degree in International Relations from SUNY New Paltz.



## Jared Melillo

Jared Melillo is a strategic intelligence leader with nearly 15 years of experience navigating the intersection of national security, global threats, and corporate intelligence. From serving in the U.S. Army and leading intelligence missions supporting the National Security Agency to directing global intelligence initiatives for Fortune 500 corporations, his career reflects the evolving role of intelligence beyond traditional government settings. A University of Arizona alumnus, Jared brings a firsthand perspective on how intelligence professionals can leverage their skills to build dynamic, impactful careers across a diverse range of industries and sectors.

# About the Speakers



## Emma Murray

Emma Murray is an Account Executive at Hetherington Group (HG), a firm specializing in investigations, intelligence, and security consulting. She began her career at The Walt Disney Company in 2021, where she served as an Investigations Analyst with Disney Corporate Security. She then transitioned into security operations as a Security Specialist with Walt Disney World Security. In 2024, she joined HG as an Intelligence Analyst, conducting research and analysis for corporate clients, before moving into her current client-facing role in 2026. Today, Emma works with organizations nationwide to understand their security and privacy needs and build tailored programs, drawing on her analytical background to connect clients with the right intelligence solutions.



## Lachlan Galbraith

Lachlan Galbraith is a Business Area Lead at Rincon Research Corporation and an Adjunct Professor of Practice with the University of Arizona's Institute for Intelligence and Information (IIO).

A retired U.S. Air Force Senior Noncommissioned Officer with 20 years of military service, Lachlan has extensive experience supporting the Department of Defense (DoD) and Intelligence Community (IC) across both tactical and strategic levels. His career spans intelligence operations, mission integration, advanced technology development, and leadership of multidisciplinary teams addressing complex national security challenges.

In his current role, he leads technical and operational initiatives focused on delivering innovative capabilities to the warfighter and intelligence professional. As an educator, Lachlan is passionate about bridging the gap between academia and operational practice, helping students understand the evolving intelligence landscape and preparing them for meaningful careers in national security.

COLLEGE OF ENGINEERING
Intelligence Operations

# STAY CONNECTED

## Follow Intelligence Operations

Instagram

Website

Facebook

YouTube

LinkedIn

## Stay in the Know

Department News • Events • Student Opportunities • Program Updates

intelligenceoperations.engineering.arizona.edu

COLLEGE OF ENGINEERING

# Intelligence Operations

**STAY CONNECTED**

**Visit our website for the latest news, events and opportunities.**