WINTER 2024
VOL 5, ISSUE 4

DEAD DROP

The Future is Now - Signals Intelligence and EW

Deep Dive: National Security Implications of High-Efficiency Batteries

Fall 2024 / Spring 2025 Course Schedule and Catalog

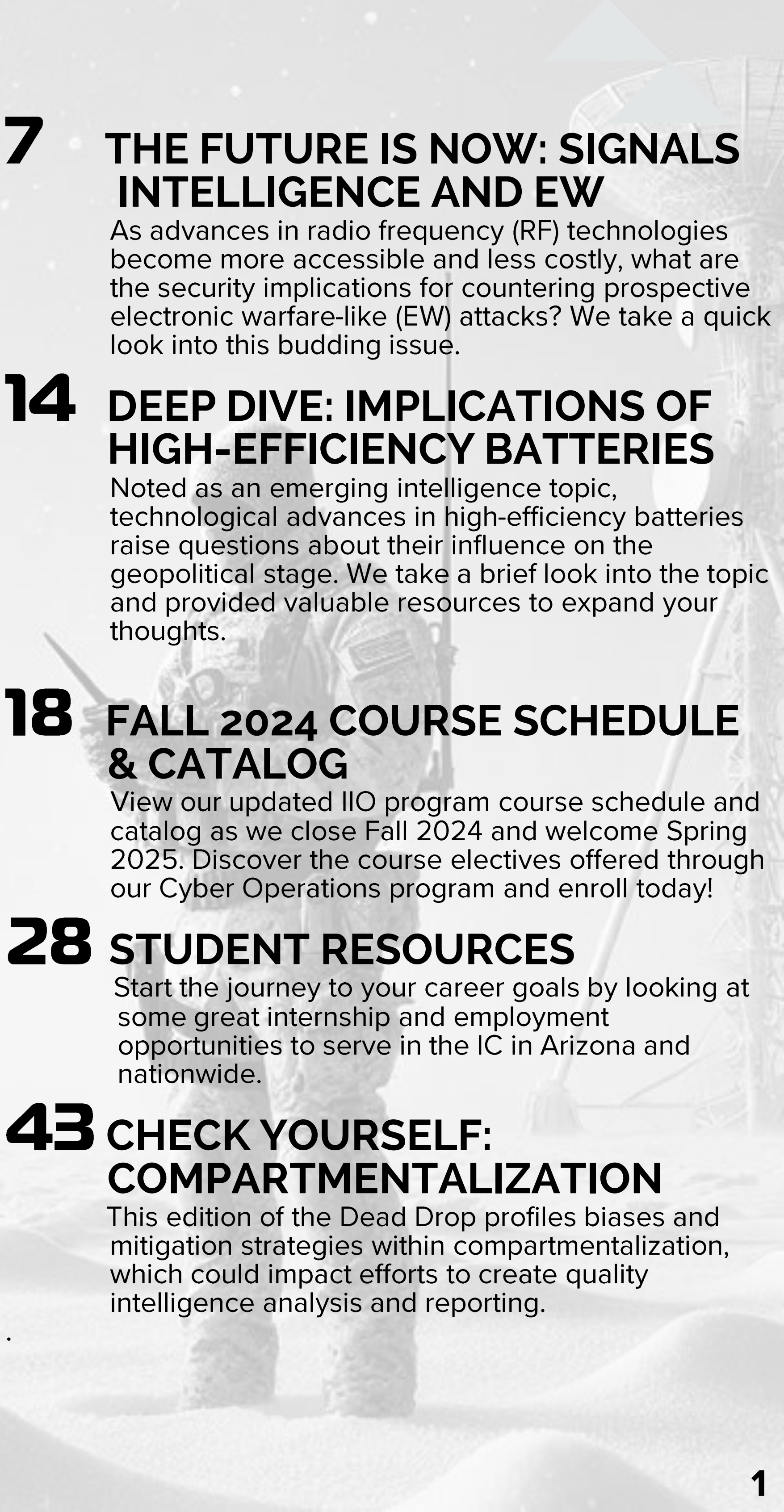
IC Scholarships, Internships & Job Opportunities

College of Applied Science & Technology

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

WHAT IS INSIDE...

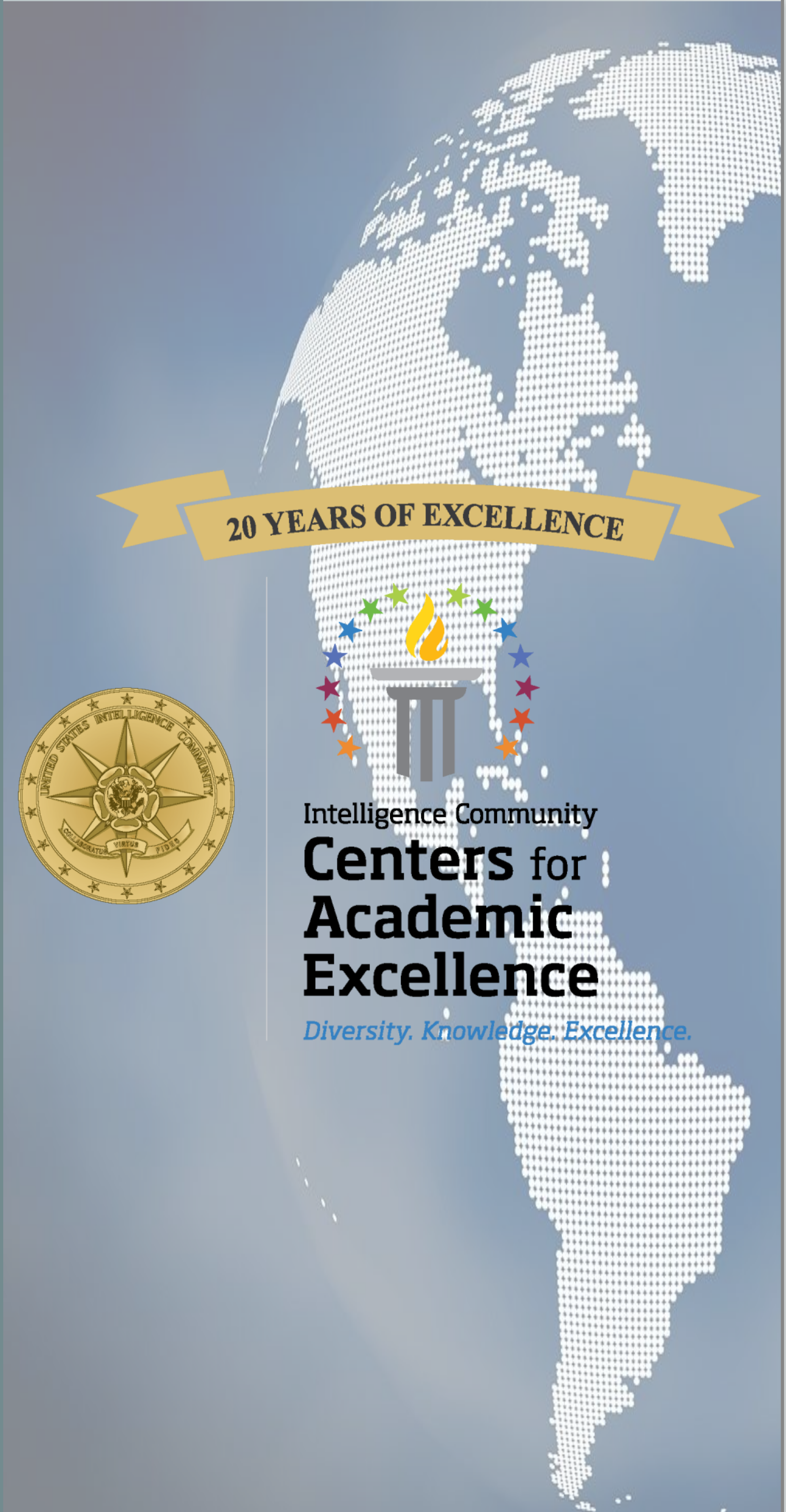
DEAD DROP



College of Applied Science & Technology

Intelligence Community Centers for Academic Excellence

Diversity. Knowledge. Excellence.



DEAD DROP

WINTER 2024 VOLUME 5 · ISSUE 4

THE UNIVERSITY OF ARIZONA
College of Applied Science and Technology
1140 Colombo Ave
Sierra Vista, AZ 85635
(520) 458-8278 (520) 626-2422 (Tucson)
azcast.arizona.edu

Facebook: @UarizonaCAST
Instagram: @uarizonacast
Twitter: @UarizonaCAST
LinkedIn: @UArizonaCAST

Managing Editor/Art Director:
Charles Walker

Special Thanks to Our Contributors: Craig Nazareth, Dalal Alharthi, Angela Lucero

ON THE COVER

The cover for our Winter Edition depicts an mobile intelligence collector in a snow field, scanning for high-value intelligence targets of the day. Even on the clearest day, the weather can make or break a sensor's ability to obtain quality signal intelligence. A special thanks to SIGINT collectors who brave the elements to ensure various tactical and strategic intelligence successes.
Photo: OpenAI

THE CORNER

INTELLIGENCE AND THE EVER-CHANGING BATTLEFIELD

As the holiday season approaches, I want to take a moment to extend my warmest wishes to each of you. This is a time for gratitude, reflection, and connection with loved ones—a chance to pause and recharge as we prepare for the opportunities and challenges.

While the holidays invite a spirit of joy and giving, they also provide a valuable opportunity for meaningful reflection. As future leaders, innovators, and contributors to the intelligence community, this season offers the perfect backdrop to think critically about the issues shaping our world and the responsibilities inherent in the work of intelligence.

Here are a few thought-provoking areas worth pondering as you navigate various discussions in your classes:

1. Ethics in Intelligence

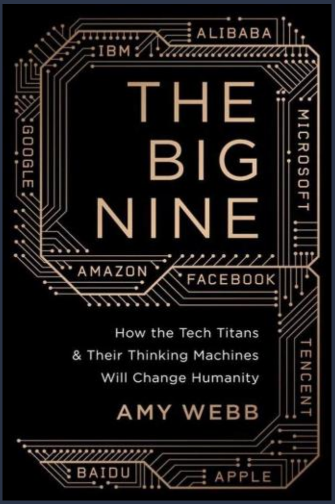
- How do we balance the pursuit of security with preserving civil liberties? What frameworks guide ethical decision-making in intelligence work?

Suggested Reading: "The Ethics of Spying: A Reader for the Intelligence Professional" by Jan Goldman Carnegie Council on Ethics in International Affairs

2. Technological Advancements

How are the recent advancements in AI, quantum computing, and cybersecurity reshaping intelligence operations? What risks and opportunities do these technologies present?

Suggested Resources: Center for Strategic and International Studies (CSIS) Technology and innovation; "The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity" by Amy Webb



3. Global Threat Landscapes

What emerging global threats should intelligence professionals prioritize? How do shifting geopolitical dynamics impact intelligence strategies?

Suggested Reading: "The Future of Power" by Joseph S. Nye, Council on Foreign Relations (CFR) Global Conflict Tracker

HAPPY HOLIDAYS
THE UNIVERSITY OF ARIZONA
College of Applied Science & Technology

BECOME AN INTELLIGENCE COMMUNITY SCHOLAR

Identify your topic
To create a stunning presentation, it's best to simplify your thoughts. Start with an outline of topics and identify highlights, which can be applied to whatever subject you plan on discussing.

EASTERN ARIZONA COLLEGE

THE UNIVERSITY OF ARIZONA

ESTRELLA MOUNTAIN COMMUNITY COLLEGE
A MARICOPA COMMUNITY COLLEGE

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

EXCELLENCE STARTS HERE.

WHY BE AN IC SCHOLAR?

IC Scholars are sought after by the U.S. Intelligence Community and receive hiring preference for government jobs. Specifically, IC Scholar graduate applications through USAJobs and IC Careers will be given more points than non-graduates , much like veterans are given more points more than non-veterans. The designation also sets graduates apart in the corporate sector.

ARIZONA ICCAE CONSORTIUM

The Arizona Intelligence Community Center for Academic Excellence (ICCAE) Consortium is a pipeline from high school through community colleges and into the University of Arizona. After graduation, highly-qualified graduates have a natural pathway to a job in the intelligence community. Estrella Mountain Community College and Eastern Arizona College are flagship Arizona ICCAE schools each with degree programs that provide a pathway to finishing your four-year degree and a career into the IC.

ESTRELLA MOUNTAIN COMMUNITY COLLEGE
A MARICOPA COMMUNITY COLLEGE

EASTERN ARIZONA COLLEGE

estrellamountain.edu

eac.edu

BENEFITS OF BEING AN IC SCHOLAR

- Selective entry into special internships
- Access to select Intelligence Community hiring events
- Preference for study abroad opportunities
- Competitive designation sets you apart for a corporate career

LEARN MORE

ciio@arizona.edu

Phone: (520)626-2442 ext. 2120

The Future is now

Signals Intelligence and EW

by CRAIG NAZARETH

This article aims to raise awareness of the value of studying electrical engineering and wired/wireless communications concepts related to Signals Intelligence (SIGINT) and Electronic Warfare (EW). The future of "democratized" SIGINT and EW is here, and we all should be more aware of the opportunities and threats these capabilities pose in our information environment.

At no time has more information been made publicly available and accessible to everyday users than today. The main drivers, such as the rapid adoption of digital technologies and increased online activity, are apparent. According to numerous studies, the ability of humans or algorithms to create content using at-your-fingertips social media and digital video platforms has led to a significantly faster growth rate in data creation and transfer (Statista, link, link). In parallel, another contributor to the massive growth in data is the growth in computing and infrastructure capability to support it, such as artificial intelligence, cloud and energy infrastructure, and satellite communications enabling relatively secure data management and access across the globe and in space.

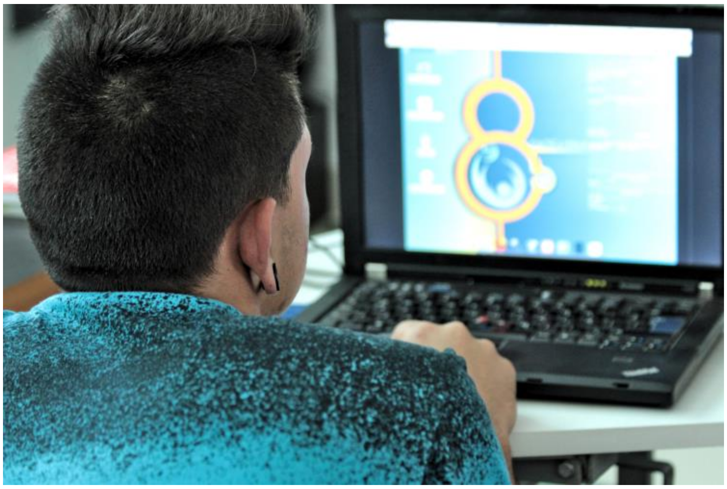
Likewise, we are witnessing a renaissance in SIGINT and EW, driven by the availability and effectiveness of sophisticated radio equipment that can fit in your hand and is powered by software you can download for free or purchase for a modest fee. These systems can intercept and exploit radio frequency (RF) signals in real-time, a feat previously only achievable by a select few with the means and know-how to deploy these capabilities (a nod to all the air, maritime, ground, and space sensor players and amateur radio operators out there). Few had the means to deploy systems that could detect signals with peak precision and clarity or attack the RF sources before breaking the power bank. For example, a SIGINT system can consist of cheap (less than $500 antennas, Software Defined Radio (SDR) hardware, and open-source SDR applications like GNU Radio). So, what does this renaissance mean for the average person or our students?

GNU Radio, Photo: Rondeau Research (Public Domain)

We all should be more interested in the opportunities and threats in this field, especially our IIO and cyber students. The common thread regarding the creation and use of content and the exploitation of that content is the electromagnetic spectrum or EMS. The EMS is all around us. It is pure energy traveling at or near the speed of light. The great minds of the past and present, like Isaac Newton, James Clerk Maxwell, Heinrich Hertz, Guglielmo Marconi, Nikola Tesla, and Hedy Lamarr, have given us the keys to fully leverage its power for encrypted communications, SIGINT, and EW. Their discovery and applied science work have led to developing sensors and systems that can detect and exploit RF signals and affect radio transmissions and equipment depending on the user's goals. These capabilities have a shallow barrier to entry.

RAND published the timely "SIGINT for Anyone" in 2017, acknowledging the sheer growth of publicly available signals intelligence capabilities previously available only to governments. Weinbaum, Berner, and McClintock explain that their "…team explored four technology areas where nongovernmental SIGINT is flourishing: maritime domain awareness; radio frequency (RF) spectrum mapping; eavesdropping, jamming, and hijacking of satellite systems; and cyber surveillance." (RAND, 2017, link). We arrive at the same conclusions in this short article, which should raise alarms for everyone. These capabilities are not only commercially available for legal applications but also illegal applications. They describe this as the "democratization" of SIGINT; these capabilities are available and accessible to anyone willing to pay for them and employ them to advance their interests or goals.

From an opportunity perspective, there are burgeoning careers across commercial, non-profit, and government spaces. RF devices and systems, including antennas, radios, and software, require engineers and analysts to employ them effectively. These systems require intelligence personnel, AI programmers, communications experts, engineers, cyber security specialists, and others to analyze and make sense of the data, identify threats that undermine data and system integrity, and test and deploy these systems to maintain reliable, protected communications. Also, there are exciting research fields related to the exploitation and use of radio frequency signals, and there is a push for expanding the efficient use of EMS, even into infrared and other electro-optic and higher frequency capabilities.



Student attends workshop to learn GNU /Linux 8 software, Photo: Niamfrifruli, CC BY-SA 4.0 via Wikimedia Commons

From a threat perspective, that low barrier of entry is also a boon to adversarial actors, including individual and networked state and non-state actors. Our reliance on Wi-Fi and Bluetooth for encrypted communications has created markets for cheap but robust RF intercept and jamming technology, including RF device scanners and jammers that scan for and can jam any RF energy, including cellular, television broadcast, Bluetooth, and Wi-Fi. Online markets sell office jamming devices to disrupt cell phone usage in local spaces for less than $100. You can buy quite capable RF scanners for less than $50. State and non-state actors are wielding these capabilities, and this growth in technology has given state actors an even more reliable and adaptive link for employing proxy forces to achieve their ends and objectives.

DIY RF Device with Jamming and Anti-jamming Capabilities, Photo: Digikey

The widespread use of digital technologies provides threat actors with a direct avenue of approach to individuals and networks with minimal cost and with a nearly negligible footprint. Russia, China, Iran, and North Korea, including criminal and terrorist organizations, have demonstrated an increasing appetite for proxy force employment and clandestine transactions to further their agendas because of this easily accessible and widely used domain. They can wield algorithmic warfare (Suchman, 2020, pp175-187, link), leveraging computers as proxies, bots, and personas to conceal the actor's intent and capability or obfuscate attribution to the responsible parties. Malware, including ransomware, is deployed by anonymous users worldwide and targets hundreds of users daily.

In conflict, the RF spectrum availability allows threat and friendly actors to augment conventional forces like ground armies, and air and sea assets with EW, cyber teams, and other unconventional forces to disrupt communications, navigation, and fire control, surveil and attack targets from hundreds of miles away, and use autonomous assets from Earth and space. Knowledge of the EMS and the propagation of radio waves, coupled with skills in system employment, is essential to optimizing these capabilities, so the demand continues to grow for people with these skillsets.

One could ask, but why now, and what has changed? There's nothing new. Savvy DIYers and governments have been harnessing the power of wired and wireless devices to communicate, eavesdrop, and interfere with other communications using RF technologies for almost 100 years. As we discussed earlier, the advent of and rapid advancement and integration of digital technology has allowed us to leverage more of the EMS to send even more packets of data across the globe.

More advanced electronics let us send and receive vast amounts of data with low power. The advancements in how we "squeeze" data into radio waves (also called modulation and encoding) also allow us to boost signal strength without a comparatively significant boost in energy required (lower power) to transmit the intended signal above the noise in our environment. The signal-to-noise ratio (SNR) is valuable when planning SIGINT or EW operations. SNR is the ratio between the signal we intend to transmit and the environmental noise. A higher SNR translates to a cleaner signal. Understanding SNR allows operators to calibrate systems to scan the RF signals based on what we expect to find in the environment. It also enables EW systems to generate RF energy (noise) in proportion to the signal EW operators are attempting to attack, even if they are low-power signals with a low probability of detection.

Our goal in the intelligence field is to detect and identify signals in our environment to drive effective operations. This requires targeted information collection to answer intelligence requirements and proactive planning so we can employ suitable sensors at the right place and time to support various operations, including EW. Preparing our environment, or in other words, analyzing how the different actors in an area are using the EMS, can pay dividends for intelligence and information operations, including SIGINT, cyber, and EW. This preparation can provide timely insights into adversarial entities' tactics, techniques, and procedures, providing opportunities to improve SIGINT and EW.

SIGINT and EW operators can insert themselves within or near the RF emission sources or transmit RF energy from afar into the radiation beam of a transmitting antenna to detect or affect the source of RF radiation. Since RF devices are developed for widespread usage in most cases, and there are technical standards and public documents that define the operating characteristics of these devices, SIGINT and EW planners can analyze an area and assess the types of devices used to make some valuable estimations to inform SIGINT collection and EW operations.

Cell towers are placed everywhere, sometimes only a mile apart, due to the heavy usage of high-frequency RF communications. Communications towers still need multiple antennae use, and amplifiers to catch the small signals transmitted by our low-power devices (5G patch antennas are highly directional and only a few square feet in size, but they must be mounted high to avoid interference with other devices and noise. Wi-Fi antennas are low-power, so they are deployed in local areas). Satellite transmissions are governed by specific standards and regulations for broadcasting telemetry data and other information.

But there is so much more to unravel with our signals. Demand for more data has driven a demand for digital signal transmission at higher frequencies—higher-energy frequency signals can send more data. Still, since these are higher-frequency signals, the wavelengths are very short (less than 1 meter in length, down to several hundred millimeters in size). Signals with very high frequencies and very small wavelengths are more susceptible to atmospheric absorption over long distances, so the SNR could drop rapidly. The RF system we select must be optimized based on the need.

Users requiring a long-range line of sight and beyond the line-of-sight (over the horizon of the Earth) communications may value a transmitting RF system that transmits in lower frequencies instead of a much higher frequency broadcast that is much more directional and more line of site. Lower frequencies with wavelengths in the hundreds of meters and kilometers tend to travel much farther but are more susceptible to interference from other RF signals and physical objects. Today, more complex modulation and encoding techniques with digital data improve SNR even at lower frequencies.

Regardless of the methods used to transmit RF energy, various measurements help us develop signatures of RF emitters and associate those signatures with threat equipment and tactics. A signature is a fingerprint. It comprises different points or measurements, like frequency and wavelength, as we already mentioned, phase, amplitude, bandwidth, polarization, direction of propagation, SNR, etc. Other measurements are depending on the depth of analysis needed. With only a partial look at the signatures most concerning to SIGINT/EW practitioners, we can assemble the puzzle to answer our requirements: what was transmitted, when was it transmitted, from where, by whom, and why? We'll explore these concepts in our next issue of the *Dead Drop* and invite our students to send us any questions or comments they have concerning this article or any related topic.

Verizon 5G repeater MMWave antenna in local Virginia neighborhood – a potential RF target, Photo: Daderot (Public Domain)

OFFICE of INTELLIGENCE and ANALYSIS

Homeland Threat Assessment

2024

DOWNLOAD ASSESSMENT

SOLVE THIS CRYPTOGRAM

NATIVE AMERICAN HERITAGE MONTH

”RYPDSEPDR BCDJPR JCD OERDC SMJX OJKEXT.”

- Black Elk

Medicine Man, Oglala Lakota Tribe

“S _ _ _ T _ _ _ S   _ R _ A _ S   A R _   _ _ S _ R
R Y P D S E P D R   B C D J P R   J C D   O E R D C

T _ A N   _ A _ _ N _ .”
S M J X   O J K E X T

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J											F		X				C	R	S						

ANSWER ON PAGE 35

National Security Implications of

HIGH-EFFICIENCY BATTERIES

Gaining a competitive edge in high-efficiency battery technology is increasingly critical for both economic and strategic reasons. As global industries shift toward clean energy and sustainable solutions, the demand for advanced batteries, particularly lithium-ion and solid-state options, is surging. These batteries are essential for powering electric vehicles, renewable energy storage, and consumer electronics. A country or company leading in this technology stands to control a significant portion of the energy storage market, reduce dependency on fossil fuels, and create job opportunities in high-tech manufacturing. For example, countries like China have heavily invested in battery production and raw material sourcing, securing a substantial portion of the global battery supply chain.

Beyond economic benefits, advancements in battery technology have substantial implications for energy security and national defense. More efficient batteries mean longer-lasting, lightweight power sources that are crucial for military equipment and operations. Maintaining leadership in this field ensures a secure supply of critical technology and reduces the strategic vulnerabilities that arise from relying on foreign sources.

Collaboration across government, industry, and academia can accelerate innovation and foster a skilled workforce. By focusing on high-efficiency battery technology, countries and companies position themselves at the forefront of a pivotal industry.

DIVE DEEPER

Collaboration and Standardization Are Key to DOD's Battery Strategy, Meeting U.S. Energy Objectives

Biden-Harris Administration Takes Further Action to Strengthen and Secure Critical Mineral Supply Chains

Department of Energy - National Blueprint for Lithium Batteries

Strauss Center - Is U.S. Dependence on China for the Battery Supply Chain a National Security Risk?

US lithium production: A vital pillar of national security and energy independence

Prioritizing battery storage to bolster US national security

INTEL IN THE NEWS

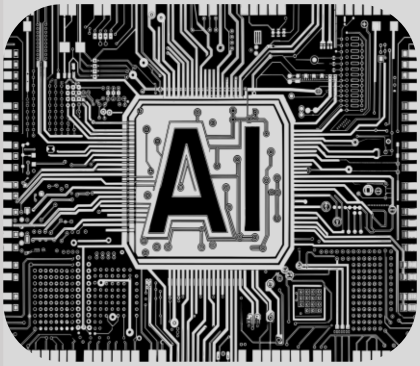
FBI Directs Calls China 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure

During a discussion on global threats, FBI Director Christopher Wray warned national security and intelligence experts and students that risks the government of China poses to U.S. national and economic security are "upon us now"—and that U.S. critical infrastructure is a prime target.

However, he suggested that partnerships with both the private sector and academia can be powerful tools in neutralizing this threat. FBI News

Russia uses Mexico as a hub for spying on the U.S.

Russians are building their presence in Mexico, targeting the United States, a return to Cold War tactics by an increasingly aggressive regime, according to U.S. officials and former intelligence officers. Russia's actions in Mexico reflect a more aggressive posture by its intelligence services across multiple fronts, as the Kremlin seeks to silence critics abroad, undermine support for Ukraine, and weaken Western democracies. U.S. and European officials add that the approach has included sabotage and attempted sabotage in Europe, assassination plots, cyberattacks, and global disinformation campaigns. **NBC News**



OpenAI launches AI chatbot for US intelligence agencies

According to a Fortune analysis, U.S. defense and security forces are stocking up on artificial intelligence, enlisting hundreds of companies to develop and safety-test new AI algorithms and tools.

The Department of Defense has awarded roughly $670 million in contracts to nearly 323 companies to work on various AI projects. The figures represent a 20% increase from 2021 to 2022 in companies working with the DOD and the total value of the contracts. Fortune

VENONA
NORTH BUILDING
'40
'50
'60
'70
SELECTED ESTIMATES ON THE SOVIET UNION 1950-1959
The CIA and the U-2 Program 1954-1974
AT COLD WAR'S END

THE VENONA PROJECT
CODED TACTICS OF A COLDER WAR

The Venona Project was a top-secret counterintelligence initiative launched by the United States in 1943, aimed at intercepting and decrypting Soviet intelligence communications. Cryptanalysts worked tirelessly on complex Soviet codes, uncovering extensive espionage activities across American institutions.

Venona uncovered the names of Americans who were passing sensitive information to the Soviet Union, including the identities of Julius and Ethel Rosenberg who passed nuclear secrets to the Soviets led to their trial and eventual execution in 1953. Other significant figures identified included Alger Hiss, a high-ranking government official, and several scientists and engineers within key U.S. defense and atomic research projects. These discoveries validated suspicions of Soviet infiltration at the highest levels and highlighted vulnerabilities in U.S. security during the early Cold War period.

The Venona Project was declassified in 1995. and ultimately played a critical role in shaping Cold War intelligence tactics, leading to greater security and counterintelligence measures within U.S. government agencies.

Project Venona Cryptanalyst Team, 1945 (Public Domain)

FBI arrests Judith Coplon, the first person arrested for espionage based on intelligence from the Venona Project (Public Domain)

MESSAGE FROM YOUR ACADEMIC ADVISORS

Confirm Your Assigned Academic Advisor

Knowing who you can contact for support is essential whether you're a newly admitted student or a continuing student. Continuing students, your academic advisor may have changed from the one you worked with in previous semesters. To check who your assigned advisor is, follow the steps below!

1. **Log into your Student Center portal on the UAccess webpage.**
2. **. Click on the Advising menu option at the top of the page and select "View Advisors," or follow the links below to find your appropriate Advisor.**

ADVISORS

CERTIFICATE ADVISORS

3. **You will see your current advisor's name, their contact information, and a link to schedule an appointment.**

Confirm Your Enrollment

Please log into your UAccess Student Center and confirm your Winter 2024 or Spring 2025 enrollment. If you have holds you are unsure about or questions about the courses you're enrolled in or are not currently enrolled in, reach out to your Advisor.

Please feel free to contact our main number at 520-621-8219 and email address at CASTAdvising@arizona.edu

IIO SCHEDULE & COURSE CATALOG

FALL 24 /SPRING 25 SEMESTER

COURSE SCHEDULE

FALL 2024

SEVEN WEEK - FIRST

CAT#	COURSE	PROFESSOR
CYBV354*	Principles of Open-Source Intelligence	McCary, John
CYBV437*	Deception, Counter-Deception & Counterintelligence	Graff, Jared
CYBV440*	Digital Espionage	Cota, Casey
CYBV450*	Information Warfare	Giordano, Joseph
INTV305	Introduction to IIO	Allen, Brent
INTV326	Introductory Methods of Intelligence Analysis	Phillippi, Emilee
INTV350	Intelligence Collection	Nazareth, Craig
INTV353	Geospatial Intelligence	Zsambok, Billy
INTV377	Psychological Operations	Longley, Carrick
INTV459	Intelligence, Surveillance, and Reconnaissance Synchronization	Wisecup, Tyler

SEVEN WEEK - SECOND

CAT#	COURSE	PROFESSOR
CYBV351*	Signals Intelligence and Electronic Warfare	Cota, Casey
CYBV354*	Principles of Open-Source Intelligence	McCary, John
CYBV450*	Information Warfare	Giordano, Joseph
INTV305	Introduction to IIO	Allen, Brent
INTV326	Introductory Methods of Intelligence Analysis	Phillippi, Emilee
INTV350	Intelligence Collection	Galbraith, Lachlan
INTV455	Target-Centric Analysis	Nazareth, Craig
INTV459	Intelligence, Surveillance, and Reconnaissance Synchronization	Wisecup, Tyler

15 WEEK

CAT#	COURSE	PROFESSOR
INTV493	Internship Study Abroad	Denno, Jason
INTV498	Senior Capstone in IIO (Section 101)	Nazareth, Craig
INTV498	Senior Capstone in IIO (Section 103)	Nazareth, Craig

* Courses offered as electives

COURSE SCHEDULE

SPRING 2025

SEVEN WEEK - FIRST

CAT#	COURSE	PROFESSOR
CYBV354*	Principles of Open-Source Intelligence	Hetherington, Cynthia McCary, John
CYBV437*	Deception, Counter-Deception & Counterintelligence	Graff, Jared
CYBV450*	Information Warfare	Giordano, Joseph
INTV305	Introduction to IIO	Allen, Brent
INTV326	Introductory Methods of Intelligence Analysis	Phillippi, Emilee
INTV350	Intelligence Collection	Nazareth, Craig Galbraith, Lachlan
INTV353	Geospatial Intelligence	Zsambok, Billy
INTV459	Intelligence, Surveillance, and Reconnaissance Synchronization	Wisecup, Tyler

SEVEN WEEK - SECOND

CYBV351*	Signals Intelligence and Electronic Warfare	Cota, Casey
CYBV354*	Principles of Open-Source Intelligence	McCary, John
CYBV450*	Information Warfare	Giordano, Joseph
INTV305	Introduction to IIO	Allen, Brent
INTV326	Introductory Methods of Intelligence Analysis	Phillippi, Emilee
INTV350	Intelligence Collection	Galbraith, Lachlan
INTV377	Psychological Operations	Longley, Carrick
INTV455	Target-Centric Analysis	Nazareth, Craig
INTV459	Intelligence, Surveillance, and Reconnaissance Synchronization	Wisecup, Tyler

15 WEEK

INTV498	Senior Capstone in IIO (Section 101)	Nazareth, Craig
INTV498	Senior Capstone in IIO (Section 103)	Nazareth, Craig

* Courses offered as electives

PROGRAM CORES

INTV 305

Introduction to Intelligence and Information Operations

Fall 2024, Seven Week – First & Second

Spring 2025, Seven Week – First & Second

Provides a broad overview of the American intelligence systems – collection, analysis, counterintelligence, and covert operations – and demonstrates how these systems work together to provide a "decision advantage" for policymakers. Students will also learn how U.S. adversaries have shifted away from directly challenging American forces and have moved to a less risky hybrid warfare model to achieve their tactical and strategic goals. Students will use a combination of research and critical thinking exercises to understand the importance of how intelligence is used to inform the decision-making process. Students will also learn to detect and guard against adversarial information operations that manipulate their sources.

INTV 326

Introductory Methods of Intelligence Analysis

Fall 2024, Seven Week – First & Second

Spring 2025, Seven Week – First & Second

Provides students with an introduction to Intelligence Analysis and instruction on how to research national security topics and incorporate tradecraft, including critical thinking and structured analytic techniques, to challenge judgments, identify mental mindsets, stimulate creativity, and manage uncertainty within the framework of providing sound assessments to decision-makers at the Strategic, Operational and Tactical level of war. Students will use scenario-based exercises to practice employing structured and other analytical techniques to answer a decision-maker's critical information requirements.

INTV 350

Intelligence Collection

Fall 2024, Seven Week – First & Second

Spring 2025, Seven Week – First & Second

This course provides students with an overview of the five U.S. intelligence Community recognized intelligence disciplines (Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Measurement and Signatures Intelligence (MASINT), and Open Source Intelligence (OSINT) to understand how to employ collection to answer information and intelligence requirements into the capabilities, limitations and applications of sensors, and discern the functional responsibilities between intelligence analysts, collection managers and decision makers across the national security enterprise.

INTV 353

Introductory Methods of Geospatial Intelligence (GEOINT)

Fall 2024, Seven Week – First

Spring 2025, Seven Week – First

This course introduces students to GEOINT operations and how intelligence professionals can incorporate tradecraft and technology to present visual depictions of critical information regarding enemy forces and terrain and provide combat operations support to decision-makers and operations planners. This course studies the electromagnetic spectrum and fundamentals of energy propagation about GEOINT systems and phenomenology. Students will be introduced to the tasking, collection, processing, exploitation, and dissemination of GEOINT systems, data, and GEOINT contributions to national security, homeland security, and strategic partnerships. This fundamental knowledge may be applied to a diverse range of constantly evolving GEOINT efforts, including support for disaster relief, force protection, and combat operations.

INTV 377

Psychological Operations

Fall 2024, Seven Week – First

Spring 2025, Seven Week – Second

This course is an introduction to the capabilities and uses of psychological operations. Students will examine psychological operations' capabilities, limitations, history, and challenges. As part of their learning experience, students will establish when psychological operations are appropriate, how to know when they have become the target of an effort to manipulate their behavior, how to mitigate their effects, and how to plan a psychological operation against a notional target. Enrollment Requirements: Students enrolled in fully online programs only.

INTV 455

Target-Centric Analysis

Fall 2024, Seven Week – Second

Spring 2025, Seven Week – Second

This course provides students with an in-depth analysis of the intelligence process, methodologies for evaluating data, threat modeling, and a process to evaluate the needs of the Intelligence consumer. Students will utilize practical analysis exercises to become familiar with threat modeling, the estimative process, and Intelligence reporting techniques to answer a decision maker's critical information requirements.

INTV 459

Intelligence, Surveillance, Reconnaissance & Synchronization

Fall 2024, Seven Week - First & Second

Spring 2025, Seven Week - First & Second

This course provides an in-depth examination of optimizing the coordination of all available collection capabilities to support intelligence operations and the military decision-making process. Students will research and engage in practical exercises to determine optimal sensor deployment schemes and sensor-to-target mix to address different collection requirements.

INTV 493

Internship Study Abroad

Fall 2024, 15 Week

This course provides students with opportunities for specialized work on an individual basis, consisting of training and practice in actual service in a technical, business, or governmental establishment.

INTV 498

Senior Capstone in Intelligence and Information Operations

Fall 2024, 15 Week

Spring 2025, 15 Week

This course provides Intelligence & Information Operations majors with a capstone experience emphasizing integrating knowledge acquired in previous classes. The course provides a culminating experience for majors involving a substantive project that demonstrates a synthesis of learning accumulated in the major, including broadly comprehensive knowledge of the discipline and its methodologies. Students are required to incorporate a field research study into their research project. This is a self-directed course where students develop and produce a senior-level research paper grounded in relevant research.

CYBV 351

Signals Intelligence and Electronic Warfare

Fall 2024, Seven Week – Second

Spring 2025, Seven Week – Second

CYBV 351 is an elective course that will provide students with an in-depth look at Signals Intelligence (SIGINT) and Electronic Warfare (EW) from a strategic, operational, tactical, and technological aspect, including the role of electromagnetic energy in SIGINT and EW operations. Students will use a combination of assessments, research, and practical exercises to gain a holistic view of SIGINT and EW applications in the National Intelligence Enterprise.

CYBV 354

Principles of Open-Source Intelligence (OSINT)

Fall 2024, Seven Week – First & Second

Spring 2025, Seven Week – First & Second

CYBV 354 provides students with an overview of the fundamentals of Open-Source Intelligence. Students will be presented with the most effective methodologies cyber professionals, law enforcement, and other investigative personnel use to locate and analyze information on the Internet and the Dark Web. Students will use interactive exercises to become familiar with the volume of sensitive data on the Internet and how it can be exploited to develop highly detailed intelligence products.

CYBV 437

Deception, Counter-Deception & Counter-Intelligence

Fall 2024, Seven Week – First

Spring 2025, Seven Week – First

CYBV437 will introduce students to deception, counter-deception, counterintelligence, and psychological operations. A survey will be presented on how these concepts are used in adversarial Information Operations and why they are among the most effective mechanisms to sway public opinion. Students will use interactive exercises to become familiar with detecting deception campaigns and the mitigation strategies to defend against them.

CYBV 450

Information Warfare

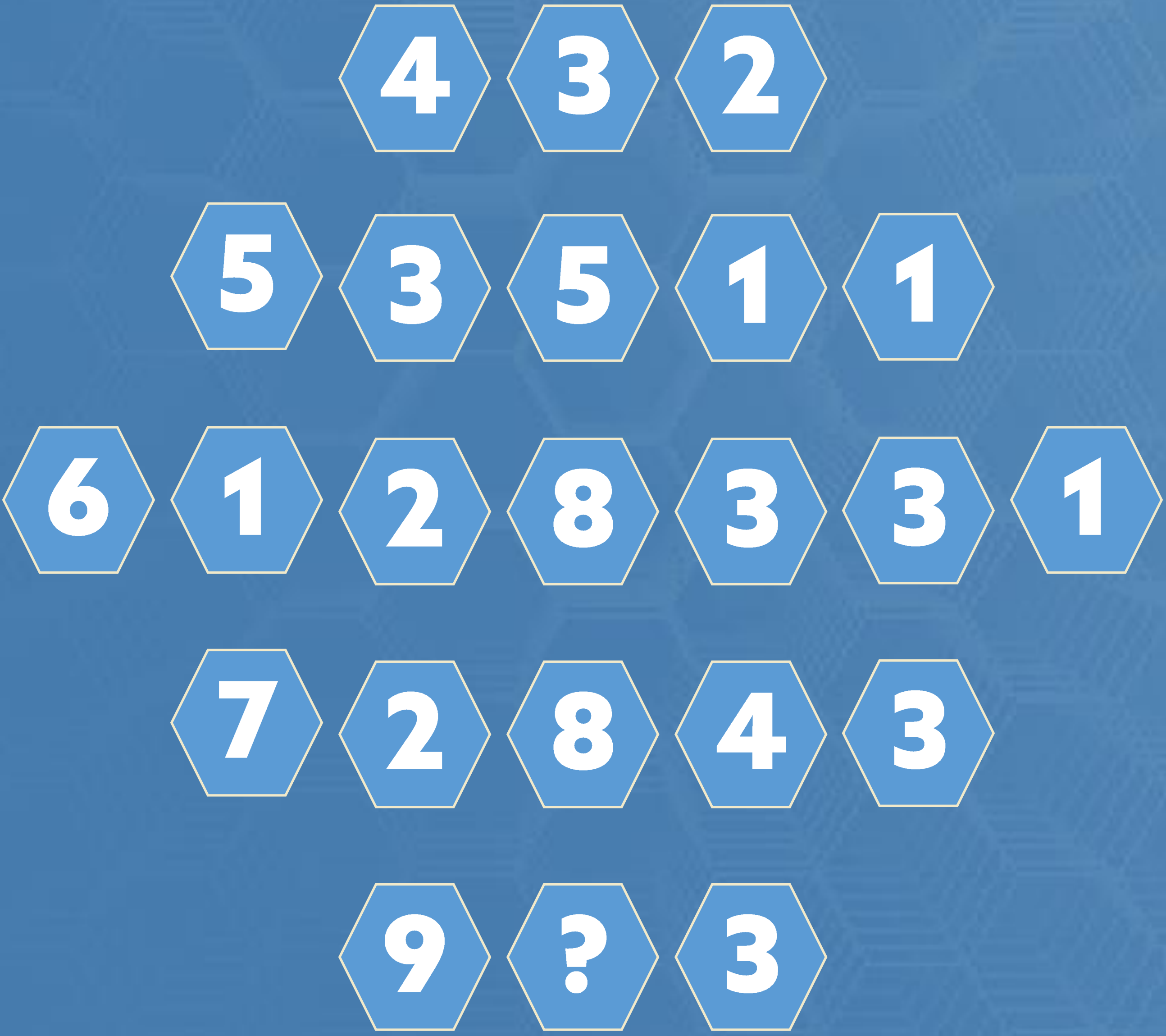
Fall 2024, Seven Week – First & Second

Spring 2025, Seven Week – First & Second

CYBV 450 will give students an in-depth overview of the tactics, techniques, procedures, and tools used to conduct and defend against Information Operation campaigns. Students will analyze case studies involving nation-state actors' online influence efforts to detect, deconstruct, and counter adversarial Information Operation campaigns.

DETERMINE THE MISSING NUMBER.

USE YOUR LOGIC SKILLS TO SOLVE THIS TEASER.



4 3 2

5 3 5 1 1

6 1 2 8 3 3 1

7 2 8 4 3

9 ? 3

ANSWER ON PAGE 35

United States Intelligence Community

Internship Opportunities for Students

To learn more, visit www.IntelligenceCareers.gov/ICStudents.html or individual IC element websites linked below

NATIONAL RECONNAISSANCE OFFICE

www.nro.gov/careers/

- Application open until July 24th, 2022 with selections typically made by October
- Paid undergraduate and graduate internship programs for summer 2023

Specific programs of interest include:

- STEM
- Economics
- Political Science
- Business Administration
- Data Science
- Human Resources
- Physical Science

DEPARTMENT OF HOMELAND SECURITY

https://www.dhs.gov/homeland-security-careers/office-intelligence-and-analysis-internship-program

- Application open from July 2022 to August 2022
- Paid undergraduate and graduate internship programs for summer 2023

Specific programs of interest include:

- Intelligence Analysis
- Health/Science
- Law Enforcement
- Technology Emergency Management
- Cybersecurity
- Public Affairs Management/Support

AIR FORCE INTELLIGENCE

https://afciviliancareers.com/paq-intel/

- Applications are currently being accepted and are accepted at various times during the year.
- Paid undergraduate and graduate 3-year internship

DEFENSE INTELLIGENCE AGENCY

https://www.dia.mil/Careers-Opportunities/Students/

- Application opens and closes at various times, typically in March the year before your internship begins
- Paid undergraduate & graduate internship programs for summer 2024

Specific programs of interest include:

- Political Science
- Global Studies
- Computer Science
- Business
- Human Resources
- Law/Criminal Justice
- Natural Sciences
- Engineering
- Logistics

OFFICE OF NAVAL INTELLIGENCE

www.oni.navy.mil/Careers/Intern-Programs/

- Application open from September 2022 to October 2022
- Paid undergraduate and graduate internship programs for summer 2024

NATIONAL SECURITY AGENCY

www.intelligencecareers.gov/nsa/nsastudents

- Application open from September 2022 to October 2022
- Paid undergraduate and graduate internship programs for summer 2023

Specific programs of interest include:

- STEM
- Computer Science
- Foreign Language
- Logistics
- Cyber Security
- Intelligence Analysis
- Information Management
- Human Resources
- Strategic Communications
- Information Technology
- Research/Development

An internship in the Intelligence Community (IC) is a great experience that can help launch your career path. Many of the opportunities highlighted here are for summer internships, but some IC elements offer internships during the academic year or that could span many years. Upon graduation and successful completion, some internships lead to non-competitive conversion to full-time employment

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

United States Intelligence Community

Internship Opportunities for Students

To learn more, visit www.IntelligenceCareers.gov/ICStudents.html or individual IC element websites linked below

Virtual Student Federal Service (VSFS)

https://vsfs.state.gov/apply

- Apply in July 2022 for an internship during the upcoming academic year
- VSFS is an unpaid, remote internship which requires no security clearance

The Presidential Management Fellowship (PMF)

www.pmf.gov

- The application is open from 13 September until 27 September
- Only graduate students (MA, PhD, JD, MBA, etc) who graduated between September 13, 2020, and September 13, 2022, or will graduate before August 31, 2023, may apply.
- Selected PMFs will have the opportunity to apply to positions across the federal government, including within the IC

CENTRAL INTELLIGENCE AGENCY

https://www.cia.gov/careers/student-programs/

- Applications accepted year-round for most programs: apply one year before preferred start date
- Paid undergraduate and graduate internship programs

Specific programs of interest include:

- Political Science
- STEM
- Education/Training
- Economics
- Information Management
- Data Science
- Media Analysis
- Cyber Security
- Computer Science
- Library Science
- International Relations
- Graphic Design
- Cartography
- Human Resources

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

DEPARTMENT OF STATE

https://careers.state.gov/interns-fellows/student-internships/

- Application opens in the fall on USA Jobs (typically opens and closes in September)
- Paid undergraduate and graduate internship for summer 2023
- Positions in many bureaus, including the Bureau of Intelligence and Research (INR)

Specific programs of interest include:

- **Student Internship Program**: opportunities to work in U.S. Embassies and Consulates throughout the world
- **Pathways Internship Program**: opportunities to explore federal careers
- Numerous Fellowship Programs
- Workforce Recruitment Program for disabled persons

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

https://www.intelligencecareers.gov/NGA/ngastudentprograms.html

- Application closes in September 2022
- Paid undergraduate and graduate internship programs for summer 2023
- Positions based in Virginia & Missouri

Specific programs of interest include:

- Business
- Geophysics
- Human Resources
- Earth Sciences
- Intelligence Analysis
- STEM
- Geography
- Finance
- Computer Science
- Social Sciences

FEDERAL BUREAU OF INVESTIGATION

www.fbijobs.gov/students

- Application opens in September 2022
- Paid undergraduate and graduate internship programs for summer 2023
- Internships offered in Washington DC as well as at many of the FBI's field offices across the country

Specific programs of interest include:

- Honors Internship Program
- Visiting Scientist Program

The Department of Energy

www.energy.gov/careers/student-recent-graduates

Three internship programs of interest:

- **Minority Educational Institution Student Partnership Program (MEISSPP)**- Typically apply by March for a paid internship. ***Learn More***.
- **DOE Scholars Program**- Typically apply by September for this internship with opportunities around the country as well as a stipend. ***Learn More***.
- **National Nuclear Security Administration Graduate Fellowship Program (NGFP)**- Apply by Early October 2022 for this paid opportunity. ***Learn More***.

U.S. Army Cyber Command

https://bit.ly/3nU0JEw

- Applications are currently being accepted and are accepted at various times during the year.
- Apply for paid positions over the summer or for 2-year fellowship opportunities
- Positions located at Fort Gordon, Georgia

Tips on Securing an Internship

1. Read the eligibility requirements before applying to ensure that you are eligible for the internship.
2. Write a federal resume. Work with your university career office and your IC CAE Program to understand the content required for a top-tier federal resume.
3. If an application requires a cover letter, tailor it to the position. This is your opportunity to connect your education and unique experience and skills to the position.
4. Be proactive and move quickly. Check often for internship openings as some agencies cap the number of applications they will accept.
5. A background investigation is typically required and some agencies also require a medical exam, foreign language, and/or military service.

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

Intelligence Analyst Internship

New Haven, CT or Remote

Description

Founded by a small team of intelligence analysts, SafeAbroad is a security consulting firm delivering intuitive intelligence and risk management solutions to our clients in the international education field. We have a startup mindset and thrive on the ingenuity of analytical thinkers. We are seeking candidates for the Intelligence Analyst (Intern) position to help us deliver actionable intelligence, risk, and safety reports to our clients. Intelligence analyst interns are expected to contribute 8-10 hours per week. The analyst shall perform the following duties:

- Enhance a data-driven risk framework to evaluate international safety concerns that have the ability to impact travelers abroad, particularly American students. Identify sources that publish open-source data on international risks (including but not limited to crime statistics, indicators of civil unrest/protests, infrastructure reliability, transportation safety, threat of terrorism, and sentiment towards Americans).
- Conduct country-level research and draft reports that highlight the area's primary safety risks to students abroad.
- Establish travel safety best practices, risk mitigation strategies, and incorporate new concepts into pre-departure guidance materials.
- Monitor news feeds and open sources for worldwide incidents that could potentially impact the safety of travelers.
- Administrative tasks, research projects, and other duties as assigned.

Requirements

- Minimum 3.0/4.0 overall GPA
- 15+ credits completed in a degree program related to national security, intelligence studies, international relations, regional or global studies, risk management, political science, journalism, social sciences, criminal justice, or information/data sciences
- Experience locating authoritative studies, reports, and databases published by the United Nations, World Health Organization, INTERPOL, and other international sources
- Experience researching foreign countries in-depth and preparing culturally sensitive written reports
- Strong command of analytic writing with the ability to convey complex information concisely and eloquently
- Strong internet research skills with advanced literacy of PowerPoint, Word, and Excel or GSuite
- Ability to manage multiple tasks and communicate project status reports to management

To Apply

Please send your resume to Recruitment@SafeAbroad.org with the Subject: "Intelligence Analyst Internship"

SAFEABROAD

SafeAbroad.com
Travel Risk Management for International Education

470 James Street, Suite 007
New Haven, CT 06513

U.S. Customs and Border Protection (CBP) Internship Program

CBP seeks high-performing University of Arizona students in the Intelligence Information and Operations (IIO) Program to seasonally support the Southern Border Intelligence Center (SBIC).

Students will assist the Executive Director in coordinating meetings, compiling deliverables, engaging with other senior leaders across the southern border, and conducting tasks as needed. This position allows selected candidate(s) to participate in intelligence planning at various strategic and operational support levels across the U.S. Government. Read more on the details on the next page.

Purpose of the Internship:

Selected applicants will have the unique opportunity to delve into intelligence. They will learn how to conduct research, form analytical conclusions, make critical judgments, and perform a variety of analytical techniques to answer key intelligence questions. The internship will provide a comprehensive understanding of the intelligence cycle, Intelligence Community Standards, and the complex border security environment.

Internship Available: Summer – Yes Fall – Yes Spring – Yes

Deadlines: To ensure your application is considered, please note that applications must be received by the first week of the previous semester. For example, if you're interested in an internship starting in the Spring semester, please submit your application within the first week of the previous Fall semester.

Agency Minimum Qualifications:

- You must be a U.S. Citizen to apply for this position
- Males born after 12/31/1959 must be registered with Selective Service
- Primary U.S. residency for at least three of the last five years
- Background Investigation: CBP is a federal law enforcement agency that requires all applicants to undergo a thorough background investigation before employment to promote the agency's core values of vigilance, service to the country, and integrity. During the screening or background investigation process, you will be asked questions regarding any felony criminal convictions or current felony charges, the use of illegal drugs (e.g., marijuana, cocaine, heroin, LSD, methamphetamines, ecstasy), and the use of non-prescribed controlled substances, including any experimentation, possession, sale, receipt, manufacture, cultivation, production, transfer, shipping, trafficking, or distribution of controlled substances. For more information, visit this link.

Agency Preferred Qualifications:

- Current University of Arizona student within good standing, with a minimum of **3.0 GPA.**
- Students in their 2nd or 3rd year of study in an Intelligence, Criminal Justice, or National Security related field

Internship Description: Unpaid (Potential to earn college units/credits)

- Providing support to senior leadership that informs and enhances their ability to make strategic decisions;
- Providing support to senior-level engagements on a variety of intelligence programs and activities;
- Assisting with the management of intra-office relationships across multiple intelligence organizations.

To Apply:

Please submit a resume, school transcript, and a writing sample (2-5 pages) to lillian.abril@cbp.dhs.gov.

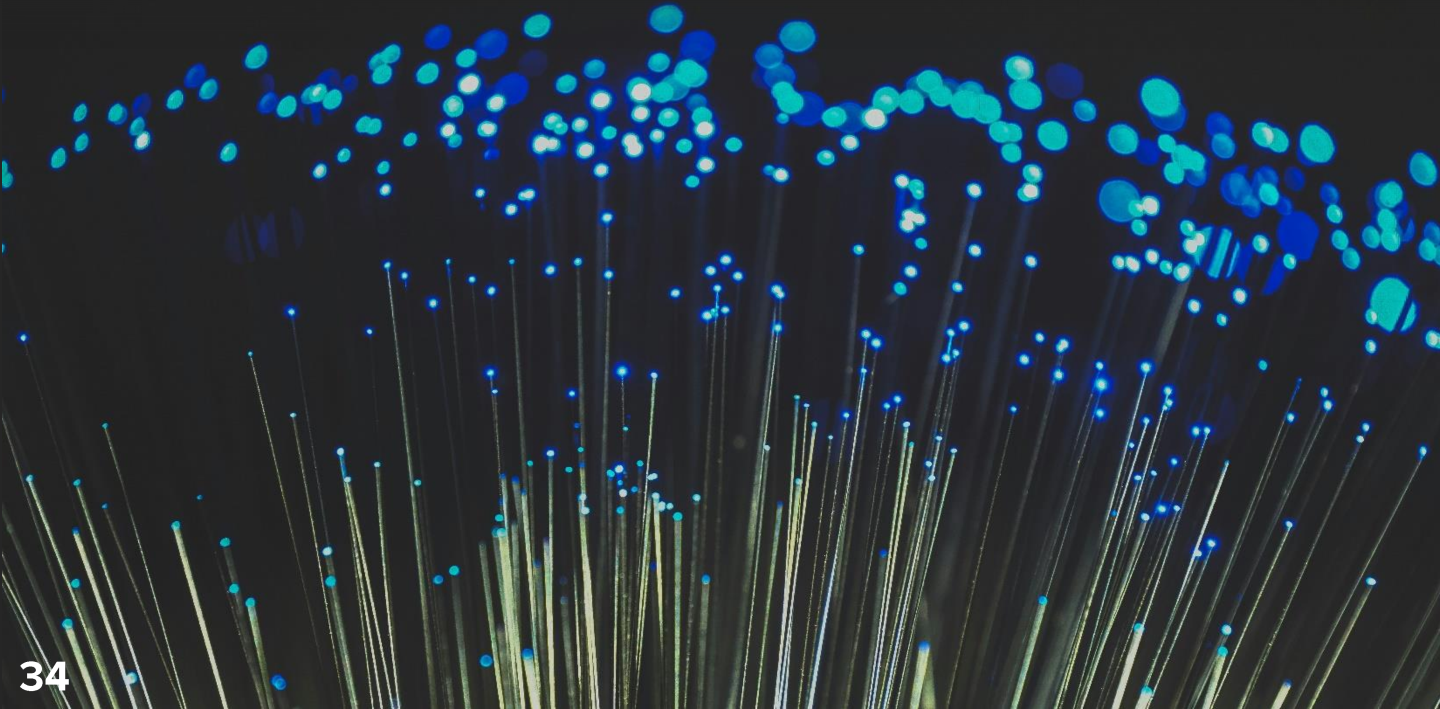
Expected Contact:

We will email you within 3-5 business days of receiving your application to set up an in-person interview.

CIA Directorate of Analysis Fellows Program

Central Intelligence Agency (CIA) Directorate of Analysis offers fellowships for undergraduate and graduate students attending four-year Minority Serving Institutions (MSIs). As an Intelligence Analyst Intern for CIA, you will work on teams alongside full-time analysts, studying and evaluating information from all available sources—classified and unclassified—and then analyzing it to provide timely and objective assessments to customers such as the President, National Security Council, and other U.S. policymakers.

Application Deadline: 6-12 months before the intended start date. Follow here for more on this unique opportunity.



RUTGERS
Center for Critical Intelligence Studies

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

The Center for Critical Intelligence Studies, a federally designated Intelligence Community Center for Academic Excellence (IC CAE), partners with numerous academic and federal institutions to provide students with various research opportunities. CCIS partners with numerous academic and federal institutions to provide research opportunities for students within the Rutgers Consortium. These opportunities fulfill the research requirement in the CIS minor as well as individual research and professional development interests. (NC Lab Opportunity is now open to **ALL IC CAE Universities/ Colleges students**.)

Spring 2025 Research Fellowships - Open Now for Applicants!

Learn more and Apply

U.S. DEPT OF DEFENSE

SMART

SCHOLARSHIP FOR SERVICE

The SMART Scholarship-for-Service Program is a combined educational and workforce development opportunity for STEM students. SMART offers scholarships for undergraduate, master's, and doctoral students pursuing a STEM degree. SMART offers two scholarship opportunities, the SMART Scholarship and the Ronald V. Dellums Memorial SMART Scholarship. All scholarship recipients receive full tuition, annual stipends, internships, and guaranteed civilian employment with the Department of Defense after graduation.

Applications are open annually from August 1 to the first Friday in December. Check your eligibility to see which scholarship you qualify for and watch our informational webinar recording for more program details.

Application Deadline: December 6, 2024 **Apply Today!**

Homeland Security Professional Opportunities for Student Workforce to Experience Research 2025

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate Office of University Programs sponsors the Professional Opportunities for Student Workforce to Experience Research (HS-POWER) Program for undergraduate and graduate students.

Benefits:

- Weekly Stipend - $750 Undergrad | $950 Graduate
- Housing Allowance - $400/week or Virtual
- Allowance - $50/week
- Inbound/Outbound Travel funds of up to $1,000

Qualifications:

- U.S. Citizenship Required
- Must be 18 Years of Age
- Must have a Cumulative GPA of 3.00 or Higher
- Be majoring in a STEM field which includes social sciences

Application Deadline: December 15, 2024

Apply Today!

women in CYBERSECURITY

WiCyS

Follow Us on Social Media

Let's Get Connected for Our Latest News & Updates

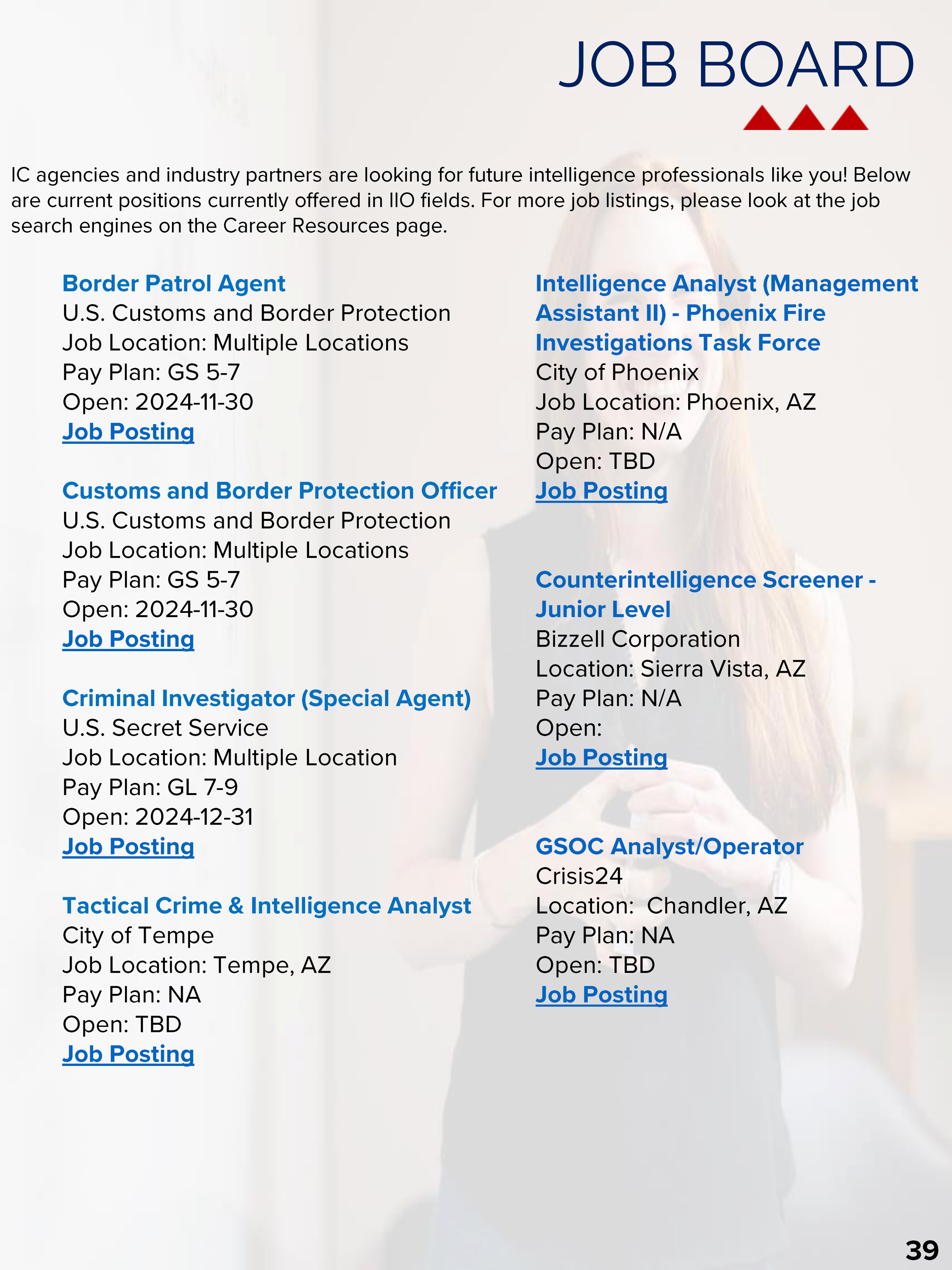
- in www.linkedin.com/company/uarizona-wicys/
- www.twitter.com/UWicys
- f www.facebook.com/UAZWicys
- www.instagram.com/uarizonawicys/

THE UNIVERSITY OF ARIZONA

WiCyS women in cybersecurity

UNIVERSITY OF ARIZONA
STUDENT CHAPTER

JOB BOARD



IC agencies and industry partners are looking for future intelligence professionals like you! Below are current positions currently offered in IIO fields. For more job listings, please look at the job search engines on the Career Resources page.

Border Patrol Agent
U.S. Customs and Border Protection
Job Location: Multiple Locations
Pay Plan: GS 5-7
Open: 2024-11-30
Job Posting

Customs and Border Protection Officer
U.S. Customs and Border Protection
Job Location: Multiple Locations
Pay Plan: GS 5-7
Open: 2024-11-30
Job Posting

Criminal Investigator (Special Agent)
U.S. Secret Service
Job Location: Multiple Location
Pay Plan: GL 7-9
Open: 2024-12-31
Job Posting

Tactical Crime & Intelligence Analyst
City of Tempe
Job Location: Tempe, AZ
Pay Plan: NA
Open: TBD
Job Posting

Intelligence Analyst (Management Assistant II) - Phoenix Fire Investigations Task Force
City of Phoenix
Job Location: Phoenix, AZ
Pay Plan: N/A
Open: TBD
Job Posting

Counterintelligence Screener - Junior Level
Bizzell Corporation
Location: Sierra Vista, AZ
Pay Plan: N/A
Open:
Job Posting

GSOC Analyst/Operator
Crisis24
Location: Chandler, AZ
Pay Plan: NA
Open: TBD
Job Posting

CAREER RESOURCES

Industry employers, partners, contractors, and federal agencies are looking for the best candidates to fill many critical positions in the Intelligence Community. Find your new career using these trusted job search engines.

U.S. Intelligence Careers

Great resource to research jobs throughout the Intelligence Community seeking various intelligence and information analysis skills. You can also find the latest scholarships and internships offered year-round.

> intelligencecareers.gov

Indeed

One of the most trusted job search engines in the nation! You will be able to find many job postings that serve many sectors of the intelligence industry. Indeed, also offers a resume uploader where you can store your pre-produced resume for easy application submissions.

> indeed.com

Clearancejobs/ Clearedjobs.net

Both sites offer pathways to employment for those students that currently hold an active or current security clearance. Most jobs listed are for federal and contract positions. Create and account and search these offerings.

> clearancejobs.com
> clearedjobs.net

USAJOBS

Widely known and respected job search tool. Find job listings with various government sectors in and out of the Intelligence Community. In addition, this site offers the ability to draft both federal and standard resumes through its internal resume builder.

> usajobs.gov

LinkedIn

One of the most effective ways to find employment is through your professional network. LinkedIn has become the industry standard social platform to connect professionals with industry leaders and hiring managers. Create your profile, engage and communicate with colleagues and recruiters, and plan your new future today!

> https://www.linkedin.com

Puzzle Answers

Solve This Cryptogram: *Phrase: "Sometimes dreams are wiser than waking." – Black Elk*

Brain Games: 6

Handshake

Talent, Meet Opportunity.

Get hired. Apply for jobs and internships offered on campus, in your local area or across the nation.

Get discovered. Stand out among your peers to reach employers actively recruiting Wildcat candidates.

Get connected. Build social networks with peers for tips to land your desired job or internship.

Get involved and make an impact. Discover on-campus and virtual career-focused training events.

arizona.joinhandshake.com

login with your NetID and password

The University of Arizona

WE WANT YOU FOR THE SOC

Join the UofA's Security Operations Center today for a rewarding, for credit, cybersecurity intern experience!

What Will You Do As A SOC Intern?

INVESTIGATION

Review vulnerability data, and record and track IT security incidents, including:
- Compromised Accounts
- Phishing
- Abuse reports

CORE OF THE INTERNSHIP

OPERATIONS

Get hands-on experience with security tools and practices within a professional business environment:
- SIEM
- IPS
- Netflow

EXPERIENCE THE SOC WORKFLOW

HUNTING

Perform threat hunting to detect and eradicate threats using various paid and open source intelligence tools!

LEARN AND USE OSINT SKILLS

This internship is available to be taken **for credit** with advisor approval and provides opportunities to develop your skills as a professional in the industry.

Interested? Apply Now On Handshake:

https://app.joinhandshake.com/emp/jobs/8260025

MINIMUM Qualifications & PREFFERED Experience

- Located in **Tucson, Arizona**
- Access to **reliable internet connection** and **computing resources**
- **Internship** is available for **credit** — with **advisor approval**
- **15-25 hours** per week **Mon-Fri || 9a -> 5pm**
- Must be a **current UofA student** studying **Cyber Operations**, **Computer Science**, or **related degree**

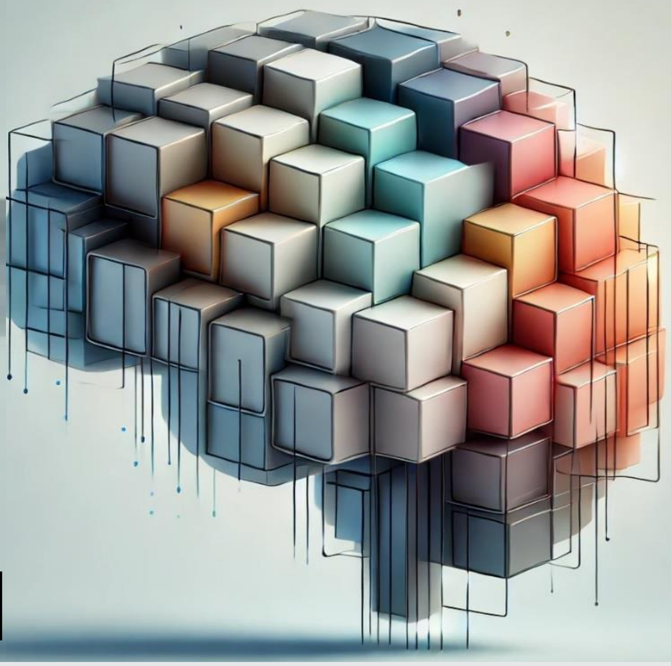
- The **Incident Handling Process**
- **Networking** (TCP/IP, UDP, DNS, DHCP, HTTP, etc.)
- **Security technologies** and **concepts** (Firewalls, Network Intrusion Detection systems, SIEM, CIA Triad)
- **NIST** Cybersecurity Framework
- Common **data analysis** tools and techniques
- Understanding of **Information Security best practices** at a **individual** and/or **organizational** level

Questions or concerns?
Email: **security@arizona.edu**

Information Security

check yourself!

MITIGATING OUR BIASES TO BECOME BETTER INTELLIGENCE PROFESSIONALS



COMPART MENTAL IZATION

Compartmentalization is a cognitive bias that occurs when information is divided into isolated "compartments," preventing intelligence professionals from seeing a cohesive or complete picture. In the intelligence community, compartmentalization is often necessary for security; information is restricted to avoid unauthorized access and protect sensitive details. However, professionals may draw incomplete or inaccurate conclusions when they view isolated information without context from other areas. This bias can lead to "tunnel vision," where analysts focus too narrowly on the information within their compartment without connecting it to broader intelligence or patterns, potentially missing critical insights.

Compartmentalization can significantly impact intelligence operations. For example, different agencies may collect pieces of intelligence that, if combined, reveal a threat. When these pieces are compartmentalized, the complete danger may not be identified in time, as no single compartment holds all the necessary information. This bias contributed to missed warnings before events like the September 11 attacks, where isolated intelligence across agencies wasn't integrated until it was too late. Overcoming compartmentalization bias is essential for accurate intelligence analysis, as it ensures a more holistic approach to decision-making and threat assessment. To mitigate compartmentalization bias, intelligence professionals can implement several strategies:

1. Encourage Cross-Agency Collaboration: Regular communication and collaborative sessions across agencies can help break down informational silos. Creating environments for shared analysis—within security limits—enables intelligence professionals to see different facets of a situation.

2. Structured Analytic Techniques (SATs): Techniques such as link analysis or hypothesis generation can help analysts visualize relationships between isolated pieces of information, fostering a more comprehensive view of data across compartments.

3. Red Team Exercises: By assigning an independent team to analyze the intelligence from an outsider's perspective, agencies can uncover gaps or alternative interpretations that compartmentalization might otherwise obscure. This approach brings fresh perspectives that can reveal overlooked connections or threats.

DEAD DROP

1140 N. Colombo Ave
Sierra Vista, AZ 85635
(520) 458-8278
(520) 626-2422 from Tucson
azcast.arizona.edu

College of Applied
Science & Technology

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