THE UNIVERSITY OF ARIZONA®

New Academic Program Workflow Form

General

Proposed Name: Information Warfare

Transaction Nbr: 00000000000078

Plan Type: Specialization

Academic Career: Undergraduate

Degree Offered: Undergraduate Certificate

Do you want to offer a minor? N

Anticipated 1st Admission Term: Sprg 2021

Details

Department(s):

UAZS

DEPTMNT ID	DEPARTMENT NAME	HOST
2910	College of Applied Science and Technology	Y

Campus(es):

DIST

LOCATION	DESCRIPTION
CHANDLER	Chandler
YUMA	Yuma

ONLN

LOCATION	DESCRIPTION
ONLN	Online

SOUTH

LOCATION	DESCRIPTION
DOUGLAS	Douglas
MESA	Mesa
NOGALES	Nogales

LOCATION	DESCRIPTION
SIERRAVSTA	Sierra Vista

Admission application terms for this plan: Spring: Y Summer: Y Fall: Y

Plan admission types:

Freshman: N Transfer: N Readmit: N Graduate: Y

Non Degree Certificate (UCRT only): N

Other (For Community Campus specifics): N

Plan Taxonomy: 29.0207, Cyber/Electronic Operations and Warfare.

Program Length Type: Program Length Value: 0.00

Report as NSC Program:

SULA Special Program:

Print Option:

Diploma: Y Undergraduate Certificate, Information Warfare

Transcript: Y Undergraduate Certificate, Information Warfare

Conditions for Admission/Declaration for this Major:

-Minimum 2.5 GPA
-Complete all pre-requisite coursework

Requirements for Accreditation:

n/a

Program Comparisons

University Appropriateness

The Information Warfare Certificate is designed to provide students in related fields with the opportunity to earn a certificate in a fast-growing and highly desired career field. Currently, the only undergraduate degree in the area of information warfare offered at the University of Arizona is the BAS in Intelligence & Information Operations (BAS-IIO) offered by the College of Applied Science & Technology (CAST). Students who take this certificate may decide to pursue an advanced degree in cybersecurity, such as the MS in Cybersecurity that is being jointly offered by MIS and ENGR or may pursue the graduate certificates in MIS or ENGR, or in the MS in Information, MS in Journalism, MS in communication and MA in International Security Studies being offered by SBS¿ thus benefiting other units on campus. Moreover, degree and non-degree seeking students could earn the certificate by taking the six required INTV and CYBV courses. UA is expanding its corporate partnerships and this certificate is appropriately designed to support their needs as well as the needs of the Department of Justice (DOJ), Department of Defense (DoD), media and communications outlets, and other governmental and non-governmental partners.

Arizona University System

NBR	PROGRAM	DEGREE	#STDNTS	LOCATION	ACCRDT

Peer Comparison

see attached

Faculty & Resources

Faculty

Current Faculty:

INSTR ID	NAME	DEPT	RANK	DEGREE	FCLTY/%
14705340	Christopher Hilliard	2910	Assit. Prof. Pract.	Master of Arts	1.00
22071416	Jason Denno	2910	Instructor	Master of Science	1.00
22074078	Thomas Jewkes	2910	Assit. Prof. Pract.	Master of Science	1.00
22078226	Paul Wagner	2910	Assit. Prof. Pract.	Master of Science	1.00
22081465	Harry Cooper	2910	Adj. Assit. Prof	Master of Science	1.00
22081483	Troy Ward	2910	Adj. Assoc. Prof	Master of Science	1.00
22081494	Jordan Vanhoy	2910	Assit. Prof. Pract.	Master of Science	1.00
22083351	Chester Hosmer	2910	Assit. Prof. Pract.	Bachelor of Science	1.00
22084985	Craig Nazareth	2910	Assit. Prof. Pract.	Prof Science Masters	1.00
22086398	Steven Wood	2910	Adj. Assit. Prof	Master of Science	1.00
22086399	Colin Brooks	2910	Adj. Assit. Prof	Master of Science	1.00
22086411	Michael Galde	2910	Assit. Prof. Pract.	Master of Science	1.00
22088393	Jonathan Martinez	2910	Adj. Assit. Prof	Master of Science	1.00
22088394	Michael Duren	2910	Adj. Assit. Prof	Master of Science	1.00

Additional Faculty:

none

Current Student & Faculty FTE

DEPARTMENT	UGRD HEAD COUNT	GRAD HEAD COUNT	FACULTY FTE
2910	1081	0	14.00

Projected Student & Faculty FTE

	UGRD HEAD COUNT			GRAD HEAD COUNT			FACULTY FTE		
DEPT	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3
2910	30	50	85	0	0	0	0.00	0.00	0.00

Library

Acquisitions Needed:

none

Physical Facilities & Equipment

Existing Physical Facilities:

none

Additional Facilities Required & Anticipated:

none

Other Support

Other Support Currently Available:

CAST Cyber Operations program will directly support the certificate.

Other Support Needed over the Next Three Years:

none

Comments During Approval Process

9/11/2020 9:49 AM

PAULEWAGNER

Comments
Approved.

9/11/2020 9:50 AM

LDENNO

Comments
Approved.

9/14/2020 11:26 AM

SWIELAND

Comments
Approved for Online and Distance locations. Mesa is not approved as it is on a teach out plan and per Paul Wagner should be replaced with PimaCCEast location.

THE UNIVERSITY OF ARIZONA®

UNDERGRADUATE CERTIFICATE – ADDITIONAL INFORMATION FORM

Note: Certificate programs offered at the University of Arizona, at the undergraduate or graduate level, are not approved as eligible programs for federal student financial aid. Although students enrolled in certificate programs are not eligible for any federal student aid programs, students may be eligible for private loans, outside scholarships, and University of Arizona department funding. For more information, please see Federal Student Financial Aid Eligibility for Programs.

General Information

Proposed Title of Certificate: Information Warfare Certificate -- Undergraduate

CIP Code: 29.0207, Cyber/Electronic Operations and Warfare

Anticipated first admission term: Spring 2021

Requested by: The College of Applied Science & Technology

Program Affiliation – specify whether the UA offers an affiliated undergraduate program – the affiliated program may or may not have the same name as the proposed certificate.

Undergraduate Major in Cyber Operations
Undergraduate Major in Intelligence and Information Operations

Certificate Description: The 18-credit hour Information Warfare Certificate will prepare students to detect, deconstruct, and counter adversarial influence operations within highly complex information environments. Students will use interactive exercises to master the ability to leverage open source data to support the development of psychological and information operation campaigns. Upon completion of the certificate, students will be able to explain how influence operations focus on manipulating the psychology of targets through strategic communication; develop and employ denial of service & counter messaging strategies to mitigate adversarial IO campaigns; and synchronize the integration of information operations with kinetic and electronic warfare operations to support hybrid and unrestricted warfare.

Purpose

The Information Warfare Certificate is designed to provide students in related fields with the opportunity to earn a certificate in a fast-growing and highly desired career field. Currently, the only undergraduate degree in the area of information warfare offered at the University of Arizona is the BAS in Intelligence & Information Operations (BAS-IIO) offered by the College of Applied Science & Technology (CAST). Students who take this certificate may decide to pursue an advanced degree in cybersecurity, such as the MS in Cybersecurity that is being jointly offered by MIS and ENGR or may pursue the graduate certificates in MIS or ENGR, or in the MS in

Information, MS in Journalism, MS in communication and MA in International Security Studies being offered by SBS– thus benefitting other units on campus. Moreover, degree and non-degree seeking students could earn the certificate by taking the six required INTV and CYBV courses. UA is expanding its corporate partnerships and this certificate is appropriately designed to support their needs as well as the needs of the Department of Justice (DOJ), Department of Defense (DoD), media and communications outlets, and other governmental and non-governmental partners.

Target Audience(s)

This program serves students from across the university, and specifically those without the technical intelligence and/or cyber background necessary to be successful in the field of information warfare. The required courses are designed to build the requisite knowledge, skills, and abilities in the area of Information Warfare. Due to the pervasive nature of the influence operations and disinformation campaigns carried out by foreign adversaries, this certificate is an excellent complement to any UA cyber, intelligence, information, media studies, journalism, political, national security, sociocultural, psychology or legal-related degree programs.

This certificate meets the needs of our: Industry partners; the Department of Defense; Federal, State, and Local government agencies; and non-governmental organizations.

If a student chooses to do so, they might major in any of the degrees housed in the College of Applied Science & Technology at the University of Arizona – the certificate provides and introductory pathway into any of these degrees:

Undergraduate Major in Cyber Operations
Undergraduate Major in Intelligence and Information Operations
Undergraduate Major in Applied Computing/Network Operations

Certificate Requirements - complete the table below to list the certificate requirements, including number of credit hours required and any special requirements for completion. Certificate requirements should include sufficient units to provide a substantive program and an appropriate level of academic rigor and in no case be less than 12 units of credit.

Minimum total units required *minimum 12 units	18
Minimum upper-division units required *minimum 6 units of credit must be upper division UA coursework	18
Total transfer units that may apply to the certificate.	0
List any special requirements to declare/admission to this certificate	-Minimum 2.5 GPA -Complete all pre-requisite coursework
Certificate requirements. List all required certificate requirements including core and electives. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.). Provide email(s)/letter(s) of support from home department head(s) for courses not owned by your department.	Core: Complete 6 courses (18 units): - INTV305 Introduction to Intelligence & Information Operations (3) - INTV377 Psychological Operations (PSYOP) (3) - CYBV354 Principles of Open Source Intelligence (OSINT) (3) - CYBV437 Deception, Counterdeception & Counterintelligence (3) - CYBV450 Information Warfare (3) - CYBV481 Social Engineering Attacks and Defenses (3)

Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	none
Additional requirements (provide description)	none
Any double-dipping restrictions (Yes/No)? If yes, provide description. *A maximum of 6 units may double-dip with a degree requirement (major, minor, General Education) or second certificate.	None distinct or beyond the University max of 6 units.

Current Courses–using the table below, list all existing courses included in the proposed certificate. You can find information to complete the table using the UA course catalog or UAnalytics (Catalog and Schedule Dashboard> “Printable Course Descriptions by Department” On Demand Report; right side of screen). If the courses listed belong to a department that is not a signed party to this implementation request, upload the department head’s permission to include the courses in the proposed certificate and information regarding accessibility to and frequency of offerings for the course(s). Upload letters of support/emails from department heads to the “Letter(s) of Support” field on the UAccess workflow form. Add rows to the table, as needed.

Course prefix and number (include cross-listings)	Units	Title	Course Description	Pre-requisites	Modes of delivery (online, in-person, hybrid)	Typically Offered (F, W, Sp, Su)	Dept signed party to proposal? (Yes/No)
INTV 305	3	Introduction to Intelligence & Information Operations	INTV 305 will provide a broad overview of the American intelligence systems - collection, analysis, counterintelligence, and covert operations - and demonstrate how these systems work together to provide a "decision advantage" for policy makers. Students will also learn how US adversaries have shifted away from directly challenging American forces and have moved to a less risky hybrid warfare model to achieve their tactical and	None	Online and in person	F, Sp	Yes

			strategic goals. Students will use a combination of research and critical thinking exercises to gain an understanding of importance of how intelligence is used to inform the decision-making process as well as how to detect and guard against adversarial information operations designed to manipulate information to induce decision makers to act against their own best interests.				
INTV 377	3	Psychological Operations (PSYOP)	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 and how to mitigate its effects, and plan a psychological operation against a notional target.	None	Online and in person	F, Sp	Yes
CYBV 354	3	Principles of Open Source Intelligence (OSINT)	CYBV354 will provide students with an overview of the fundamentals of Open Source Intelligence. Students will be presented with the most effective methodologies used by cyber professionals, law enforcement, and other investigative personnel to locate and analyze information on the Internet and Dark Web. Students will use interactive exercises to become familiar with the volume of sensitive data on the Internet and how it can be	CYBV301 or INTV305 or consent of instructor	Online and in person	F, Sp	Yes

			exploited to develop highly detailed intelligence products.				
CYBV 437	3	Deception, Counterdeception & Counterintelligence	CYBV437 will provide students with an introduction to the concepts of deception, counter-deception, counterintelligence, and psychological operations. A survey of how these concepts are used in adversarial Information Operations and why they are among the most effective mechanisms to sway public opinion will be presented. Students will use interactive exercises to become familiar with how to detect deception campaigns as well as the mitigation strategies to defend against them.	CYBV301 or INTV305 or consent of instructor	Online and in person	F, Sp	Yes
CYBV 450	3	Information Warfare	CYBV 450 will provide students with 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 on Nation State actors’ online influence efforts in order to detect, deconstruct, and counter adversarial Information Operation campaigns.	CYBV301 or INTV305 or consent of instructor	Online and in person	F, Sp	Yes
CYBV 481	3	Social Engineering Attacks and Defenses	CYBV 481 will provide students with an advanced analysis of the tactics, techniques, and tools used to conduct and defend against Social Engineering attacks. A survey of why social engineering attacks are among the most effective Cyber-attack mechanisms and what can be done to mitigate them will be presented. Students will use interactive exercises to	CYBV480 or Consent of Instructor	Online and in person	F, Sp	Yes

			master social engineering attacks and defenses in order to be able to develop policies and procedures to increase organizational security posture.				

New Courses Needed – using the table below, list any new courses that must be created for the proposed program. If the specific course number is undetermined, please provide level (ie CHEM 4**). Add rows as needed. Is a new prefix needed? If so, provide the subject description so Curricular Affairs can generate proposed prefix options.

None

Faculty & Resources

Current Faculty - complete the table below. If UA Vitae link is not provided/available, attach a short CV (2-3 pages) to the end of the proposal or upload to the workflow form. UA Vitae profiles can be found in the UA directory/phonebook. Add rows as needed. Delete the EXAMPLE rows before submitting/uploading. NOTE: full proposals are distributed campus-wide, posted on committee agendas and should be considered “publicly visible”. Contact Liz Sandoval if you have concerns about CV information being “publicly visible”.

Faculty Member	Involvement
Jason Denno, MS, MBA	Cyber Operations Teaches CYBV354, CYBV437, CYBV450, and CYBV481
Paul Wagner, MS, MBA	Cyber Operations, Teaches CYBV481
Chris Hilliard, MA	Intelligence & Information Operations, Teaches INTV305, INTV377, and CYBV450
Craig Nazareth, MS	Intelligence & Information Operations, Teaches INTV305
John McCary, MS	Intelligence & Information Operations, Teaches CYBV354 and CYBV437

Additional Faculty – Describe the additional faculty needed during the next three years for the initiation of the program and list the anticipated schedule for addition of these faculty members.

None. All program growth due to increased enrollment in the Information Warfare Certificate will be addressed by the current Cyber Operations and Intelligence & Information Operations program Full Time and Adjunct Faculty.

Library Acquisitions Needed – Describe additional library acquisitions needed during the next three years for the successful initiation of the program.

None

Physical Facilities & Equipment - Assess the adequacy of existing physical facilities and equipment available for the proposed certificate. Include special classrooms, laboratories, physical equipment, computer facilities, etc. Describe additional physical facilities and equipment that will be required or are anticipated during the next three years for the proposed program.

None

Other Support - Describe other support currently available for the proposed certificate. Include support staff, university and non-university assistance. List additional staff and other assistance needed for the next three years.

None

Marketing & Recruitment - Provide a detailed and robust marketing strategy for this certificate.

1) The current Intelligence & Information Operations (IIO) program is already a robust existing program with over 175 declared majors. We have implemented a marketing plan that consists of the following:
   a. UA Intelligence & Information Operations program website located at: https://iio.azcast.arizona.edu. The IIO program website provides detailed information on: our Defense Intelligence Agency (DIA)/Office of the Director of National Intelligence (ODNI) designation as an Intelligence Community Center of Academic Excellence (IC-CAE); detailed information on our IIO BAS degree program to include sample program schedules and course descriptions/learning outcomes; the UA CyberApolis Virtual Learning Environment; Intelligence Community Career information; Intelligence & Information Operations Faculty; and admissions requirements. Our Intelligence & Information Operations program website is linked to the UA Main website and the UA admissions application website.
   b. The Intelligence & Information Operations program is also fully integrated into Arizona Online and its website located at: https://online.arizona.edu/programs/undergraduate/online-bachelor-applied-science-intelligence-and-information-operations-bs. This website provides high level details on the Intelligence & Information Operations program, our DIA IC-CAE designation, example courses, and links to admissions and the application. This site also provides links back to the UA Intelligence & Information Operations program website.
   c. CAST has also developed a one-page Intelligence & Information Operations pamphlet with high level program details and contact information for both Admissions and the Intelligence & Information Operations program office. These pamphlets are given out at various CAST Advisor and IIO program recruiting events. They are also made available on the UA Sierra Vista campus.
   d. CAST Advisors also markets the Intelligence & Information Operations program through their monthly newsletter that goes to current and prospective students.
   e. The IIO program's pre-existing partnerships with the Department of Defense, the US Intelligence Community, the National Security Administration, the Federal Bureau of Investigations, and local and domestic Industry partners provide direct promotional and marketing opportunities for the certificate at no cost to CAST. Furthermore, collaboration with the University of Arizona's Applied Research Corporation provides promotional and marketing

prospects with outside corporations.

f. Finally, the Intelligence & Information Operations program has developed a detailed web-magazine-like monthly newsletter called *The Dead Drop.* The *Dead Drop* is sent to all current, prospective, and graduated Intelligence & Information Operations students. The *Dead Drop* is also sent to all of the Intelligence Community industry, government, and transfer pathway academic partner institutions. The *Dead Drop* is a 20 to 40-page document that provides students details on: Major Intelligence related events for the month; upcoming semester course offerings; UA Spotlight on two or more of our Intelligence & Information Operations Faculty; important dates and program information; as well as information on pre-vetted scholarship, internship, and job opportunities that are available to our students.

2) We have implemented an initial student recruitment plan that consists of the following:

By means of digital and print media, radio ads, outdoor advertising such as rented billboards, news releases, direct mail, direct e-mail, website, social media, and personal outreach by the Advising Team, our promotion and communication efforts will focus on raising awareness of the value of obtaining a degree in Intelligence & Information Operations, along with generating interest in and providing information about career opportunities for Intelligence professionals. We use traditional advertising channels, which reach a wider audience, to achieve this objective, paired with making individual connections with prospective students. We make additional contact with prospective students through outreach to community colleges by meeting with community college instructors and administrators to create partnerships to streamline the options students have to transfer seamlessly from their community college program into the Intelligence & Information Operations department to complete their BAS degree. In addition, our Advising Team members hold office hours on site at the community college campuses to make themselves available to prospective students for informal visits and conversations to help examine options for credit transfer. These informal conversations augment the more formal classroom visits also conducted by the Advising Team to provide information to prospective students in a larger presentation setting. Once the students have moved beyond awareness and interest in the college, we leverage interactive communication channels to begin building a relationship and move individuals through the final stages of the decision process to move forward with applying to the University of Arizona. The objective is to raise awareness and communicate the college's value proposition to prospects, and the community at large. The goal is to drive traffic to the CAST website where visitors can search for information and begin engaging with the college. From the CAST website, students and their families can access details to reinforce the value of obtaining their degree here, from seeing the lower tuition rates available to CAST and University of Arizona Online, to learning more about the nationally-recognized caliber of the curriculum of the Intelligence & Information Operations BAS.

Financial - Provide a copy of the budget for the certificate including start-up costs and the anticipated costs for the first three years. Include some indication of how this fits with the overall department budget.

See attached

Student Learning Outcomes and Assessment – describe what students should know, understand, and/or be able to do after completing this certificate, and how student outcomes will be assessed.

In completing the Certificate, students will be able to:

- Understand and describe how tapping into the emotional component of an idea can spark a revolt
- Explain the different types of means and methods used in digital influence & manipulation operations

- Examine and evaluate and explain the differing tactics, techniques and foci of Social Engineering & Psychological Operations and how each is employed to support Information Warfare
- Scrutinize and propose how influence operations focus on manipulating the psychology of targets through strategic communication
- Assess and propose how denial of service & counter messaging strategies can be employed to mitigate an adversarial IO campaign
- Examine and propose how Information Operations can be integrated with kinetic and electronic warfare operations to support hybrid and unrestricted warfare
- Identify and describe how the principles of Influence and Manipulation can be used to trick a user into violating a security policy
- Define and explain the different types of delivery methods that can be used in a social engineering campaign
- Describe and demonstrate how seemingly legitimate files can be used to compromise a user's computer
- Identify and describe how the browser is the most dangerous avenue for malware infection
- Describe and explain the mitigation strategies that can be used to defend the human from a social engineering attack
- Describe and explain the mitigation strategies that can be used to defend the endpoint and network from a social engineering attack
- Identify and explain how Ethical Hacking and Social Engineering tests can be used to improve an organization's overall security posture
- Understand and describe the goals, capabilities, and limitations associated with Open Source Intelligence
- Examine and evaluate the different types of files that contain useful metadata as well as how to access, modify and delete metadata
- Examine and evaluate how to use web-based and proprietary open source search tools to conduct investigations
- Examine and evaluate the different image and video formats and how data can be embedded or hidden within the format
- Examine and evaluate how to conduct reverse image searches to identify the origin, modifications, and geolocation data associated with an image or video
- Examine and evaluate how to conduct Social Media research to obtain and leverage sensitive personal data during an investigation
- Examine and evaluate how to find the geolocation of an WiFi access point or a subject's IP address using Internet search tools
- Examine and evaluate how to locate and leverage government documentation to verify and validate information about a subject
- Identify and understand how the principles of deception, counter-deception, counterintelligence, and psychological operations can be used to deceive and manipulate populations and organizations
- Examine and evaluate how deception and denial campaigns are coordinated to achieve Information Warfare goals
- Examine and evaluate the basic deception principles; planning functions; and operational management tasks that are used to conduct information operations
- Examine and propose how to detect deception operations using channel management and analysis
- Examine and propose the mitigation strategies that can be used to defend against adversarial deception operations
- Examine and propose how to use deception techniques to counter Nation State Actors in Cyberspace
- Identify and analyze how the American Intelligence Community is structured
- Explain how the Intelligence Community supports "decision advantage"
- Analyze and evaluate the fundamental characteristics and capabilities of each of the Intelligence disciplines
- Analyze and evaluate why collection sources and methods must be protected
- Analyze and evaluate the differences between covert and clandestine operations
- Analyze and interpret how information operations can be used to conduct targeted data collection, content creation, and false

amplification on social media platforms

- Analyze and evaluate how Information Operations are used to support national strategic goals

Topics covered:

- Intelligence community structure; controlling authorities; and the Intelligence cycle
- Overt, Clandestine, and Covert operations
- Open Source Intelligence capabilities and limitations; collection methods; analysis methodologies; fusion with more traditional intelligence disciplines
- Physical and cyber deception techniques; counter-deception techniques; and counterintelligence techniques
- Information Operations: channels detection and monitoring; channel management; campaign amplification
- Social Engineering tactics, techniques and tools
- Psychological Operations; influence operations; civil authority leveraging and manipulation

Assessment Plan– identify factors that indicate that completion of the certificate enhances the undergraduate experience. Describe measures for programmatic assessment, and provide a detailed plan for assessing certificate outcomes.

Learning Outcomes	Sources(s) of Evidence	Assessment Measures	Data Collection Points
Outcome 1: Analyze the structure and functions of the US national security and intelligence communities, including law enforcement agencies.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of INTV305 End of CYBV450
Outcome 2: Identify and apply tactics, techniques, and procedures used to conduct and defend against Information Operation campaigns.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of INTV305 End of INTV377 End of CYBV354 End of CYBV437 End of CYBV481 End of CYBV450
Outcome 3: Demonstrate critical thinking strategies, including: reasoning, problem solving, analysis, and evaluation, through; analytic writing, application of research methods, and advanced briefing skills.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of INTV305 End of INTV377 End of CYBV354 End of CYBV437 End of CYBV450
Outcome 4: Describe and demonstrate how knowledge about an adversary's motivation, intentions, and methods are collected, analyzed, and disseminated to	Course-embedded assessments	Exams, practical exercises, & reports	End of INTV377 End of CYBV437 End of CYBV481

help security personnel to align resources within an enterprise architecture.		Comprehensive research project and report	End of CYBV450

Certificate Outcomes and Assessment– identify factors that indicate that completion of the certificate enhances the undergraduate experience. Describe measures for programmatic assessment, and provide a detailed plan for assessing certificate outcomes.

Certificate Outcomes
Factors indicating that the Certificate leads to gainful employment and/or advancement include: Offers of employment to interns* at their place of internship*, employment at a desirable position (as articulated by the student) within one year of earning the certificate, promotion in professional setting within one year of earning the certificate, and long-term satisfaction with working conditions (2, 5, and 10 years out from earning the certificate). Indication from annual surveys of our former students that the certificate was a factor in their employment success

*interns and internship are not associated with academic credit or part of a programatic offering

Assessment Plan
Certificate Outcomes will be assessed:

- Annually through an outgoing survey of Certificate Students regarding the above factors.
- Annually through a survey of employers as identified by those who earned the certificate.

Certificate Demand
Anticipated Enrollment and General Demand:
This certificate program will target:

1. Current UA students interested in augmenting their current degree program with this particular skill set
2. Returning Intelligence & Information Operations as well as returning Cyber Operations students already working in the field wanting to improve their skills and/or increase their eligibility for promotion
3. New non-degree seeking students from our corporate and government partnerships

3-Year Projected Annual Enrollment			
Projected Number of Students	**1st Year**	**2nd Year**	**3rd Year**
	30	50	85

General Demand
CAST’s existing Intelligence & Information Operations program had 66 declared majors at the end of the Spring 2019 semester. Since the announcement of the DIA/ODNI IC-CAE designation, the Intelligence Information Operations program has had 111 new admissions. The shift in the focus of the program from pure Intelligence Studies to Intelligence and Information Operations as well as the national recognition gained from the DIA/ODNI IC-CAE designation nearly tripled the program size in three semesters from 66 declared majors to over 177 for the Fall 2020 semester. Although we do not expect the program to sustain this rate of growth

into the future, we do expect strong continued growth due to the emerging need for professionals with the knowledge, skills, and abilities that this program will directly address.

The Department of Defense and its Intelligence Community partners have begun to merge their Cyber, Intelligence, and Information Operations capabilities to counter new threats who have shifted away from directly challenging US forces to a less risky hybrid warfare model. The DoD and IC are in the infancy of this transition and are still developing the tactics, techniques, procedures, and doctrine on how to operate and fight in the new operational environment. Our program was selected as the number one IC-CAE designee in the Nation by the Defense Intelligence Agency (DIA) specifically because our program addresses this need. The reason this degree program will continue to be one of the most popular programs at the CAST is that it is preparing students for an emerging career field in which the demand to fill critical positions far outweighs the number of available skilled professionals.

It is within the following strategic environment and global context that Arizona students will be positioned: Private and public organizations across the globe are operating within a dynamic and complex information environment that persists across the cyber and non-cyber domains. The sheer volume of data and information challenges these institutions face daily requires the implementation of holistic information protection, information assurance, and strategic messaging strategies to remain relevant, to counter threat narratives, and to be able to exploit strategic opportunities. The explosive growth of novel media platforms (social, political, informational, economic, technological, etc) and access to these platforms afforded by the internet, adds to the challenges, causing individuals and organizations to adapt constantly as threat actors (criminals, terrorists, nefarious governments) manipulate information to achieve their objectives. In the private sector, Harvard Business Review states that "…most companies remain badly behind the curve…" when it comes to data management and making data and information relevant for decision making. "…Less than 1% of its unstructured data is analyzed or used at all. More than 70% of employees have access to data they should not, and 80% of analysts' time is spent simply discovering and preparing data." Additionally, numerous business experts confirm that branding and messaging are a necessity to achieve a competitive advantage. In the public sector, the United States Department of Defense emphasizes that security "…depends upon the open and reliable access to information…" and that actors are "…persistently exfiltrating sensitive information from…public and private sector institutions while others are using "… cyber-enabled information operations to influence [the] population and challenge […] democratic processes."

These factors are driving demand for graduates and future employees who understand this environment and context and can support organizations as they work to improve their effectiveness and agility in this environment.

Source: Harvard Business Review. https://hbr.org/2017/05/whats-your-data-strategy
Source: 2018 Department of Defense Cyber Strategy https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Needs Served by the Certificate

The U.S. Department of Labor identifies information and security analysts, management analysts, information services management, scientific and technical consulting services, and management of companies and enterprises as key employment opportunities, which are available to Arizona graduates. Within the Department of Defense and the military writ large, USA Jobs, the primary search tool for available employment opportunities, lists numerous information warfare and data and information management positions available to prospective candidates. While many of these opportunities are available to more seasoned personnel, there are internship tracks and new hire programs available, as well as contract positions available. Median annual wages range from $98,350 (Information Security Analysts) to $156,580.

According to the Bureau of Labor Statistics,“Employment of information security analysts is projected to grow 32 percent through 2028, much faster than the average for all occupations. Demand for information security analysts is expected to be very high, as these analysts will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks. The median annual wage for information security analysts was $98,350 in May 2018.” Additionally, the Bureau states that Management Analyst positions, which include those employees contributing to strategic planning and information strategies, is projected to grow 14 percent through 2028, much faster than the average for all occupations. Demand for the services of these workers should grow as organizations continue to seek ways to improve efficiency and control costs. The median annual wage for management analysts was $83,610 in May 2018.

The media and communications industry has identified a critical gap in the capability of journalism and communications professionals to counter or mitigate the damage from the information war. In a special event hosted by the Columbia School of Journalism, they state “Good journalism is no longer sufficient to combat the assault on truth and democracy. Media companies are striving to counter the threat of information warfare by working in new and different ways, and to respond to the ethics challenges posed by this struggle.” The Information Warfare undergraduate certificate will also serve to bridge the major expertise void present in new and seasoned media and communications experts. The certificate equips the student with the knowledge, skills, and abilities to challenge state sponsored disinformation campaigns, develop solutions to detect misinformation and maintain information security and integrity in reporting.

According to the Bureau of Labor Statistics “Employment of media and communication occupations is projected to grow 4 percent from 2018 to 2028, about as fast as the average for all occupations, which will result in about 27,600 new jobs. Demand for media and communication occupations is expected to arise from the need to create, edit, translate, and disseminate information through a variety of different platforms. The median annual wage for media and communication occupations was $59,230 in May 2019, which was higher than the median annual wage for all occupations of $39,810.”

Source: www.dol.gov
Source: www.usajobs.gov
Source: https://data.bls.gov/
Source: https://journalism.columbia.edu/special-event-information-wars

Related Positions:

- Information Warfare Officer
- Social Media Analyst
- Intelligence Specialist
- PSYOP Specialist
- Deception Officer
- OSINT Analyst
- Strategic Messaging Specialist
- Civil Affairs Specialist
- Counter Cyber Threat Intel Analyst

- Threat Operations Consultant
- Cyber Operations Analyst
- Cyber Attribution Analyst
- Marketing and public relations director
- Social digital media specialist
- Account executive
- Marketing communications manager
- Strategic planning coordinator
- Business segment analyst
- Media strategist
- Media Analyst
- Communications Director

Local worksites for Information Warfare students include:

Department of Homeland Security
Fort Huachuca
Raytheon
Leidos
General Dynamics
Lockheed Martin
SAIC
Boeing
Rincon Research
Arizona Department of Public Safety
Arizona Critical Infrastructure Providers (e.g. TEP, APS, SRP, etc.)

Similar programs:

Despite the growing requirement for Information Warfare skills in both the government and commercial sectors, market research demonstrated Information Warfare programs being limited to military academies and unavailable nationally in the academic sector. Associated programs were predominately found in the areas of national security, defense studies, public administration, intelligence, international relations, and government and public diplomacy with reduced availability of related coursework in the information warfare field. Only one undergraduate degree and one graduate certificate in the communications field were identified to have related information warfare program requirements. Furthermore, the second closest degree to the information warfare field is strategic communications. However, institutions offering degrees in strategic communications or communications in general focus entirely on civil, public, private journalism, organizational management, and business management oriented communications vice national security related communications. There are several cyber related courses (network defense, cyber engineering) offered as part of BS degrees, but research revealed no programs that offer social engineering related courses, or courses and degree programs related to information warfare.

Some of the associated programs found with comparable or similar (limited) coursework nationally are:

<u>Undergraduate (Degree and Certificates)</u>

National American University - BS in Intelligence Management - Comparable program and general electives available for the BS degree
https://henley-putnam.national.edu/programs/bachelors-science-intelligence-management/

Stanford University - BA in Communications - Select related coursework in the program of study for the BA
https://exploredegrees.stanford.edu/schoolofhumanitiesandsciences/communication/#bachelorstext

Graduate Level (Degree and Certificates)

University of Texas at El Paso - Online Master of Defense and Strategic Studies - Comparable core and elective courses offered for the MDSS
https://www.utep.edu/extendeduniversity/utepconnect/online-programs/master-programs/master-of-defense-and-strategic-studies.html

The Naval Postgraduate School - Master of Science in Information Warfare Systems Engineering - Comparable program requirements
https://nps.edu/documents/103424507/106734757/698_Matrix.pdf/d8fda791-4544-4bf2-aae7-9e6b3e1d7217?t=1440709633000

The Naval Postgraduate School - Master of Science in Information Warfare Systems Engineering - Comparable program requirements
https://nps.smartcatalogiq.com/en/Current/Academic-Catalog/Graduate-School-of-Operational-and-Information-Sciences-GSOIS/Department-of-Information-Sciences/Information-Warfare-Curriculum-595

The Institute of World Politics - Masters of Arts in Statecraft and National Security Affairs - Comparable core courses and electives available for the MA
https://www.iwp.edu/degrees/master-of-arts-in-statecraft-and-national-security-affairs/

The Institute of World Politics - Graduate Certificate in Public Diplomacy & Strategic Influence - Comparable course requirements for the certificate
https://www.iwp.edu/degrees/certificate-in-public-diplomacy-and-strategic-influence/

The Institute of World Politics - Graduate Certificate in Strategic Communications - Comparable course requirements for the certificate
https://www.iwp.edu/degrees/certificate-in-strategic-communication/

International Options:

Universiti Teknologi MARA, Selangour, Malaysia - MA in Media & Information Warfare Studies - Closely related coursework psychological operations, intelligence and security studies
https://cmiws.uitm.edu.my/main/index.php/2015-08-21-02-45-45/ma-in-media-and-information-warfare-studies

Universiti Teknologi MARA, Selangour, Malaysia - Ph. D. in Media & Information Warfare Studies - Closely related coursework in psychological operations, intelligence and security studies
https://cmiws.uitm.edu.my/main/index.php/2015-08-21-02-45-45/ph-d-in-media-and-information-warfare-studies

C. Collaborations

There will be no collaborations with other departments or universities for this certificate program other than donated courses toward this program if depts. choose to do so.

Contacts and Administration
List the name and contact information for the primary point of contact for the certificate.

Jason Denno, Director - Cyber, Intelligence & Information Operations, College of Applied Science & Technology, jasondenno@arizona.edu

List the name and contact information for the person or persons who will serve in the role of Director of Undergraduate Studies (DUS) for the certificate (this is not always the same as the DUS for affiliated programs or head of the managing academic unit.)

Jason Denno, Director - Cyber, Intelligence & Information Operations, College of Applied Science & Technology, jasondenno@arizona.edu

If known, list the members of the certificate oversight committee for this certificate. *Note: undergraduate certificate oversight committees shall consist of a minimum of 3 members, 2 of which are faculty and at least one of the 2 is participating faculty in the certificate program. The oversight committee is responsible for 1)qualifications of participating faculty, 2)coordination of admissions recommendations with the Office of Admissions, and 3) curricular changes.*

Jason Denno, Director - Cyber, Intelligence & Information Operations, College of Applied Science & Technology, jasondenno@arizona.edu

Craig Nazareth, Assistant Professor of Practice – Intelligence & Information Operations, College of Applied Science & Technology, cnazareth@arizona.edu

Chet Hosmer, Assistant Professor of Practice – Cyber Operations Security Computing, College of Applied Science & Technology, chesterhosmer@arizona.edu

Undergraduate Certificate Peer Comparison Chart- Select two peers for completing the comparison chart from (in order of priority) ABOR-approved institutions, AAU members, and/or other relevant institutions recognized in the field. The comparison chart will be used to identify typically required coursework, themes, and experiences for certificate programs within the discipline. The comparison programs are not required to have the same certificate name as the proposed UA program. Information for the proposed UA program must be consistent throughout the proposal documents. Delete EXAMPLE columns once ready to submit/upload.

***NOTE:* There are no Peer Undergraduate Certificate offerings in this space. There are several graduate level programs and certificates in this area that are closely related, yet we are proposing the first undergraduate certificate in this area.**

Certificate name, institution	**Proposed UA Program:**	**Peer 1:**	**Peer 2:**
Current# of enrolled students	[redacted]	Current enrolled students statistics, completion rate statistics, nor gainful employment disclosures are available for this program.	Current enrolled students statistics, completion rate statistics, nor gainful employment disclosures are available for this program.
Certificate program description	The 18-credit hour Information Warfare Certificate will prepare students to detect, deconstruct, and counter adversarial influence operations within highly complex information environments. Students will use interactive exercises to master the ability to leverage open source data to support the development of psychological and information operation campaigns. Upon completion of the certificate, students will be able to explain how influence operations focus on manipulating the psychology of targets through strategic communication; develop and employ denial of service & counter messaging strategies to mitigate adversarial IO campaigns; and synchronize the integration of information operations with kinetic and electronic warfare operations to support hybrid and unrestricted warfare.	https://nps.smartcatalogiq.com/en/Current/Academic-Catalog/Graduate-School-of-Operational-and-Information-Sciences-GSOIS/Department-of-Information-Sciences/Information-Warfare-Curriculum-595 Graduates of this curriculum are thoroughly knowledgeable in Information Operations (IO) and Information Warfare (IW). They receive a Master of Science in Information Warfare Systems Engineering (MSIWSE) degree that provides the services with officers who are well versed in the technical, theoretical, and operational aspects of interdisciplinary IO/IW as they relate to joint mission objectives in modern warfare. This curriculum is sponsored by the Headquarters USMC, Director of Strategy and Plans.	https://www.amu.apus.edu/academic/schools/security-and-global-studies/certificate-grad/joint-warfare.html The graduate certificate in Joint Warfare is designed for students interested in the theory and practice of military operations from the mid-19th to the 20th century. You'll study joint warfare theory, practice, planning, strategy, and implementation. Special emphasis includes different dimensions of coalition warfare using case studies, while conventional and unconventional warfare is examined in light of technological change and the information age. This online program is helpful for careers in military service, government agencies, or other organizations that need experienced professionals with in-depth knowledge of warfare and its effect on national security and security threats. This online certificate is geared toward graduate students who want to expand their knowledge of joint warfare

			without committing to a degree program.
Target careers	-Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners -Large Retail and Manufacturing Companies	-Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners -Large Retail and Manufacturing Companies	-Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners -Large Retail and Manufacturing Companies
Minimum total units required	18	Completion of a minimum of 45 quarter-hours of graduate-level work, of which at least 15 hours must represent courses at the 4000 level, and in two (or more) discrete disciplines. Graduate courses in at least four discrete academic specialization sequences, minimum, and in two disciplines, a course at the 4000 level must be included. One Systems Engineering class. The candidate's program must be approved by the Chairman, Information Sciences Department.	18
Minimum upper-division units required	18	45	18
Total transfer units that may apply to certificate	None	None	None
List any special requirements to declare/admission to this certificate (completion of specific coursework, minimum GPA, interview, application, etc.)	Minimum 2.5 GPA Complete all pre-requisite coursework	A baccalaureate degree with above-average grades with courses in science and mathematics (through integral calculus) is required for entry. Additionally, applicants must have a minimum academic profile code (APC) of 324. Eligibility for TOP SECRET security clearance with access to SPECIAL COMPARTMENTED INFORMATION (SCI) is	All AMU master's degree/graduate certificate programs require a bachelor’s degree (or higher) from an institution whose accreditation is recognized by the Council for Higher Education Accreditation (CHEA).

		required for U.S. students. Applicants not meeting the mathematics requirements may be considered for entry via a refresher quarter.	
Certificate requirements. List all certificate requirements including core and electives. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.).	INTV305 Introduction to Intelligence & Information Operations (3) INTV377 Psychological Operations (PSYOP) (3) CYBV354 Principles of Open Source Intelligence (OSINT) (3) CYBV437 Deception, Counterdeception & Counterintelligence (3) CYBV450 Information Warfare (3) CYBV481 Social Engineering Attacks and Defenses (3)	IW0810 Thesis Research for IW Students (8 Lab Hours) IW3101 Military Operations in the Information Environment (4) IW4500 Information Warfare Systems Engineering (3 Lecture Hours and 2 Lab Hours) IW3921 Non-Kinetic Targeting (3) IW4960 Advanced Information Warfare Systems (3 Lecture Hours and 2 Lab Hours)	MILS514 The Making of Strategy (3) MILS560 Joint Warfare Theory and Practice (3) MILS561 Joint Warfare Planning and Implementation (3) MILS562 Joint Warfare Command and Control (3) MILS563 Case Studies in Joint Warfare (3) MILS620 Studies in Future War (3)
Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	None	Yes. In addition to the 45 graduate hours of course work, an acceptable thesis must be completed.	None
Additional requirements (provide description)	None	None	None

*Note: comparison of additional relevant programs may be requested.

THE UNIVERSITY OF ARIZONA®

BUDGET PROJECTION FORM			
Name of Proposed Program or Unit:			
	Projected		
Budget Contact Person:	1st Year 2021 – 2022	2nd Year 2022- 2023	3rd Year 2023- 2024
METRICS			
Net increase in annual college enrollment UG	30	50	85
Net increase in college SCH UG	540	900	1530
Net increase in annual college enrollment Grad	-	-	-
Net increase in college SCH Grad	-	-	-
Number of enrollments being charged a Program Fee	-	-	-
New Sponsored Activity (MTDC)	-	-	-
Number of Faculty FTE	0	0	0
FUNDING SOURCES			
Continuing Sources			
UG RCM Revenue (net of cost allocation)			
Grad RCM Revenue (net of cost allocation)			
Program Fee RCM Revenue (net of cost allocation)			
F and A Revenues (net of cost allocations)			
UA Online Revenues	$175,500	$292,500	$497,250
Distance Learning Revenues			
Reallocation from existing College funds (attach description)			
Other Items (attach description)			
Total Continuing	$175,500	$292,500	$497,250
One-time Sources			
College fund balances			
Institutional Strategic Investment			
Gift Funding			
Other Items (attach description)			
Total One-time			
TOTAL SOURCES	$175,500	$292,500	$497,250
EXPENDITURE ITEMS			
Continuing Expenditures			
Faculty	N/A	N/A	N/A
Other Personnel			
Employee Related Expense			
Graduate Assistantships			
Other Graduate Aid			
Operations (materials, supplies, phones, etc.)			
Additional Space Cost			
Other Items (attach description)			
Total Continuing	$0	$0	$0
One-time Expenditures			
Construction or Renovation			
Start-up Equipment			
Replace Equipment			

Library Resources			
Other Items (attach description)			
Total One-time			
TOTAL EXPENDITURES	$0	$0	$0
Net Projected Fiscal Effect	$175,500	$292,500	$497,250

College of Applied Science & Technology

1140 N. Colombo Ave.
Sierra Vista, AZ 85635
Tel: 520-458-8278
Fax: 520-458-5823
www.azcast.arizona.edu

To Whom It May Concern:

The College of Applied Science and Technology's Cyber Operations Program is proposing multiple cyber security undergraduate certificates. These include the following:

- Penetration Testing
- Security Computing
- Cyber Defense
- Digital Forensics
- Reverse Engineering
- Information Warfare

After conducting a local and national search for similar curriculum, it was determined that there is nothing comparable at the undergraduate level. There are no letters of support for these certificates due to this analysis.

If our search missed something or you have concerns about these certificate proposals, please reach out to me.

Thank you for your time.

Paul E. Wagner, MS, MBA
Interim Academic Dean
Department Head, Applied Technology
Assistant Professor of Practice
College of Applied Science and Technology
The University of Arizona