# Executive Summary

## Request for Authorization to Implement BAS in Cyber Operations

<table>
<thead>
<tr>
<th>Requested by</th>
<th>University of Arizona South</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP Code</td>
<td>29.0207 Cyber/Electronic Operations and Warfare</td>
</tr>
</tbody>
</table>
| **Purpose of Program**        | The BAS in Cyber Operations prepares graduates for cyber-related occupations in defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security content delivered within state-of-the-art Cyber Virtual Learning Environment to ensure students have extensive hands-on experiences to develop the knowledge, skills, and abilities necessary to succeed after graduation. The BAS in Cyber Operations offers three sub-plans, in-person and online: 1) Cyber Engineering, 2) Defense and Forensics, and 3) Cyber Law and Policy.  

The core of the BAS in Cyber Operations is designed to meet the National Security Agency requirements for designation as a Center of Academic Excellence in Cyber Operations (and is 1 of 20 schools nationwide to receive this designation), which requires students to become proficient in both offensive and defensive cyber operations.  

The major requires 42 units consisting of 27 units of shared core and 15 units of sub-plan coursework. Students are required to complete 3 units of senior capstone (CYBV 498) resulting in a senior project thesis paper.  

Upon completion of the BAS in Cyber Operations program, students will be able to:

1. Demonstrate a thorough understanding of various operating systems and be able to develop low level applications with the required complexity and sophistication to implement exploits for discovered vulnerabilities.  
2. Safely perform static and dynamic analysis of unknown software, including obfuscated malware, to fully understand the software’s functionality.  
3. Explain and demonstrate the phases of offensive cyber operations; what each phase entails; who has the authorities to conduct each phase; and how operations are assessed after completion.  
4. Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.  
5. Demonstrate and explain how to acquire a forensically sound image; understand user activity; determine the manner in which an operating system or application has been subverted; identify forensic artifacts left by attacks; and recover deleted and/or intentionally hidden information.  
6. Demonstrate a thorough understanding of how networks work at the... |
infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones.

7. Demonstrate understanding of how variability affects outcomes; how to identify anomalous events; how to integrate and differentiate continuous functions of multiple variables; and how to solve complex problems using computation and scripting languages.

8. Describe and explain the relationship between cyber ethics and law; US and International cyber laws; criminal penalties related to unethical hacking; and apply the notion of Gray Areas to articulate where the law has not yet caught up to technology innovation.

9. Demonstrate and explain the various types of vulnerabilities and their underlying causes; how security principles interrelate and are typically employed to achieve assured solutions; and explain how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.

10. Describe and demonstrate how knowledge about an adversary’s motivation, intentions, and methods are collected, analyzed, and disseminated to help security personnel and business staff to align resources and protect critical assets within an enterprise architecture.

<table>
<thead>
<tr>
<th>5-year projected annual enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt; year</td>
</tr>
<tr>
<td>300</td>
</tr>
</tbody>
</table>

**Source(s) of Funding**

- Continuing Sources:
  - UG RCM Revenue
  - Arizona Online Revenue
  - Distance Learning Revenue

**Expenditures:**

- Additional adjunct instructors anticipated if additional growth occurs. Current faculty staffing is adequate and accommodates the current growth rate, with the addition of a pending full time hire in Computer Science.

**Approvals:**

- ABOR: 2/08/2019
- Undergraduate Council: 2/12/2019
- Graduate Council: N/A
- CAAC: 12/18/2018
- Provost’s Council: 2/18/2019
- Faculty Senate: 2/18/2019
New Academic Program Workflow Form

General

**Proposed Name:** Cyber Operations

Transaction Nbr: 00000000000012

Plan Type: Major

Academic Career: Undergraduate

Degree Offered: Bachelor of Applied Science

Do you want to offer a minor?  N

Anticipated 1st Admission Term: Fall 2019

Details

Department(s):

**UAZS**

<table>
<thead>
<tr>
<th>DEPTMNT ID</th>
<th>DEPARTMENT NAME</th>
<th>HOST</th>
</tr>
</thead>
<tbody>
<tr>
<td>2910</td>
<td>University of Arizona South</td>
<td>Y</td>
</tr>
</tbody>
</table>

Campus(es):

**DIST**

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANDLER</td>
<td>Chandler</td>
</tr>
<tr>
<td>MAURITIUS</td>
<td>UA Mauritius</td>
</tr>
<tr>
<td>YUMA</td>
<td>Yuma</td>
</tr>
</tbody>
</table>

**ONLN**

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONLN</td>
<td>UA Online</td>
</tr>
</tbody>
</table>

**SOUTH**

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOUGLAS</td>
<td>Douglas</td>
</tr>
<tr>
<td>NOGALES</td>
<td>Nogales</td>
</tr>
</tbody>
</table>
**Admission application terms for this plan:** Spring: Y Summer: Y Fall: Y

**Plan admission types:**
- Freshman: N  
- Transfer: Y  
- Readmit: Y  
- Graduate: N  

**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  
- Transcript: Y

**Major in Cyber Operations**

**Conditions for Admission/Declaration for this Major:**

The Cyber Operations program requires a supplemental program application in addition to admission to The University of Arizona. The entrance requirements include:
- Minimum 2.5 GPA in your college coursework
- Resume
- Goal statement

**Cyber Engineering Subplan:**
- AAS in Cybersecurity (recommended)
- ECE 175: Computer Programming for Engineering Applications (3 units)
- BASV 300, MATH 243 or CSC 245: Intro to Discrete Math (3 units)

**Defense/Forensics and Cyber law and Policies Subplans:**
- AAS degree in cybersecurity related field (recommended)

**Cyber Engineering Subplan:**
- AAS degree in computer science related field (recommended)

**Requirements for Accreditation:**

Already designated as a center for academic excellence in Cyber Operations by
the National Security Agency. Accreditation good until 2023.

Program Comparisons

University Appropriateness

The Bachelor of Applied Science in Cyber Operations (BAS-CO) fulfills the mission of the University in several important ways. The study of Cyber Operations is a key element of the Fourth Industrial Revolution and a cutting edge discipline. The proposed BAS-CO also fulfills the land grant mission of the University by offering the program to students beyond the geographical boundaries of the University of Arizona main campus through the UA South branch campus, Distance Campus locations, and Arizona Online, and does so through an innovative, flexible, and accessible online Virtual Learning Environment. The BAS-CO prepares students for immediate employment in the growing field of Cyber Operations—a central tenet of the UA South college mission.

Arizona University System

<table>
<thead>
<tr>
<th>NBR</th>
<th>PROGRAM</th>
<th>DEGREE</th>
<th>#STDNTS</th>
<th>LOCATION</th>
<th>ACCRDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Applied Computing - Cyber Scrty</td>
<td>BS</td>
<td>27</td>
<td>Arizona State University</td>
<td>Y</td>
</tr>
</tbody>
</table>

Peer Comparison

The Bachelor of Applied Science in Cyber Operations (BAS-CO) is a program that is relatively unique compared to programs offered at other public peer institutions. There are no other bachelor degree programs of any kind in Cyber Operations offered by Arizona public institutions. There are programs in Cybersecurity and in Information Assurance offered at the University of Arizona, Arizona State University, and Northern Arizona University, but they are not comparable. The core of the BAS-CO was designed to meet the National Security Agency requirements for designation as a Center of Academic Excellence in Cyber Operations (and is one of 20 schools nationwide to receive this designation), which requires students to become proficient in both offensive and defensive cyber operations. Students in the BAS-CO learn, practice, and are assessed on many of their learning outcomes utilizing the Cyber Virtual Learning Environment, allowing them to gain knowledge and skills with real world applications in a controlled environment.

Faculty & Resources

Faculty

Current Faculty:

<table>
<thead>
<tr>
<th>INSTR ID</th>
<th>NAME</th>
<th>DEPT</th>
<th>RANK</th>
<th>DEGREE</th>
<th>FCLTY/%</th>
</tr>
</thead>
<tbody>
<tr>
<td>22071416</td>
<td>Jason Denno</td>
<td>UAZS</td>
<td>Assit. Prof</td>
<td>Master of</td>
<td>25.00</td>
</tr>
<tr>
<td>INSTR ID</td>
<td>NAME</td>
<td>DEPT</td>
<td>RANK</td>
<td>DEGREE</td>
<td>FCLTY/%</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
<td>------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>---------</td>
</tr>
<tr>
<td>22078226</td>
<td>Paul Wagner</td>
<td>UAZS</td>
<td>Assit. Prof. Pract.</td>
<td>Master of Science</td>
<td>100.00</td>
</tr>
<tr>
<td>22074078</td>
<td>Thomas Jewkes</td>
<td>UAZS</td>
<td>Assit. Prof. Pract.</td>
<td>Master of Science</td>
<td>100.00</td>
</tr>
<tr>
<td>22051906</td>
<td>Linda Denno</td>
<td>UAZS</td>
<td>Assit. Prof</td>
<td>Doctor of Philosophy</td>
<td>25.00</td>
</tr>
<tr>
<td>12104529</td>
<td>Sandra Moore</td>
<td>UAZS</td>
<td>Assit. Prof</td>
<td>Master of Science</td>
<td>25.00</td>
</tr>
<tr>
<td>14206933</td>
<td>Li Xu</td>
<td>UAZS</td>
<td>Professor</td>
<td>Doctor of Philosophy</td>
<td>12.50</td>
</tr>
<tr>
<td>22075489</td>
<td>Odile Wolf</td>
<td>UAZS</td>
<td>Assit. Prof</td>
<td>Master of Science</td>
<td>12.50</td>
</tr>
<tr>
<td>23251330</td>
<td>Ture Peken</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Doctor of Philosophy</td>
<td>25.00</td>
</tr>
<tr>
<td>22077766</td>
<td>Elke Drennan</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Doctor of Philosophy</td>
<td>50.00</td>
</tr>
<tr>
<td>22080699</td>
<td>Heidi Calhoun-lopez</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Juris Doctor</td>
<td>25.00</td>
</tr>
<tr>
<td>22077810</td>
<td>Rock Stevens</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Master of Science</td>
<td>50.00</td>
</tr>
<tr>
<td>22073944</td>
<td>Mohamed Meky</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Doctor of Philosophy</td>
<td>25.00</td>
</tr>
<tr>
<td>22076592</td>
<td>Luis Mendieta</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Master of Science</td>
<td>50.00</td>
</tr>
<tr>
<td>22080509</td>
<td>David Drennan</td>
<td>UAZS</td>
<td>Adj. Instor.</td>
<td>Master of Science</td>
<td>50.00</td>
</tr>
</tbody>
</table>

Additional Faculty:

The current faculty is adequate to accommodate the current growth rate, with the addition of a pending full time hire in Computer Science. Additional growth will be accommodated by the hiring of additional adjunct instructors.

Current Student & Faculty FTE

<table>
<thead>
<tr>
<th>DEPARTMENT</th>
<th>UGRD HEAD COUNT</th>
<th>GRAD HEAD COUNT</th>
<th>FACULTY FTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAZS</td>
<td>170</td>
<td>0</td>
<td>5.75</td>
</tr>
</tbody>
</table>

Projected Student & Faculty FTE

<table>
<thead>
<tr>
<th>DEPT</th>
<th>YR 1</th>
<th>YR 2</th>
<th>YR 3</th>
<th>YR 1</th>
<th>YR 2</th>
<th>YR 3</th>
<th>YR 1</th>
<th>YR 2</th>
<th>YR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAZS</td>
<td>200</td>
<td>275</td>
<td>350</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5.75</td>
<td>6.00</td>
<td>6.00</td>
</tr>
</tbody>
</table>

Library

Acquisitions Needed:
n/a

Physical Facilities & Equipment

Existing Physical Facilities:
Existing facilities are adequate.

Additional Facilities Required & Anticipated:
n/a

Other Support

Other Support Currently Available:
The BAS in Cyber Operations currently has a full-time program manager who supports the program in all administrative aspects. Also, the UA South Student Services office has dedicated a full-time academic advisor to the program who works closely with the program director, faculty, and program manager, with expertise in program requirements, course prerequisites, transfer pathways, etc. The program is also supported by general university support staff in scheduling, instruction design, enrollment services, etc. The Cyber Virtual Learning Environment, through which the curriculum for many of the courses is offered, is currently supported by Ephibian, a University of Arizona-affiliated software development company.

Other Support Needed over the Next Three Years:
The need for additional support is not anticipated.

Comments During Approval Process

10/10/2018 11:42 AM
EHENLEY

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>We would like sub-plans indicated on degree.</td>
</tr>
</tbody>
</table>

10/10/2018 11:43 AM
EHENLEY

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>We would like sub-plan listed on the diploma.</td>
</tr>
<tr>
<td>Date/Time</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>10/15/2018 2:02 PM</td>
</tr>
<tr>
<td>10/16/2018 6:30 AM</td>
</tr>
<tr>
<td>10/16/2018 12:54 PM</td>
</tr>
</tbody>
</table>
NEW ACADEMIC PROGRAM-UNDERGRADUATE MAJOR
ADDITIONAL INFORMATION FORM

I. PURPOSE AND NATURE OF THE MAJOR—provide a description for the proposed program. Include the purpose, nature, and highlights. The description will be displayed on the advisement report and should match departmental and college websites, handouts, promotional materials, etc.

The BAS in Cyber Operations prepares graduates for cyber-related occupations in defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure our students have extensive hands-on experiences to develop the knowledge, skills, and abilities necessary to succeed after they graduate. The BAS degree in Cyber Operations offers three subplans, both in-person and fully online: Cyber Engineering, Defense and Forensics, or Cyber Law and Policy.

II. MAJOR REQUIREMENTS—complete the table below to list the major requirements, including minimum number of credit hours, required core, electives, and any special requirements, including sub-plans, theses, internships, etc. Note: information in this section must be consistent throughout the proposal documents (comparison charts, department checklists, curricular/assessment map, etc.). Delete the EXAMPLE column before submitting/uploading. Complete table found in Appendix A if requesting a corresponding minor.

<table>
<thead>
<tr>
<th>Total units required to complete degree</th>
<th>120 Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper-division units required to complete degree</td>
<td>45 Units for students with an AAS from an Arizona Community College or the CCAF <em>Or</em> 60 Units</td>
</tr>
<tr>
<td>Foundation courses</td>
<td></td>
</tr>
<tr>
<td>Second language</td>
<td>CYBV 473—Violent Python or CSCV 352—System Programming in Unix or CYBV 470—C Programming for Security Professionals (2nd Semester Programming Language) or 2nd Semester Foreign Language Proficiency</td>
</tr>
<tr>
<td>Math</td>
<td>BASV 314—Mathematics for Applied Sciences <em>or</em> BASV376 Mathematics for Applied Technology</td>
</tr>
</tbody>
</table>
| General education requirements | TIER II GENERAL EDUCATION (21 Units)  
|                              | Natural Sciences (3 Units)  
|                              | Arts and Humanities (6 Units)  
|                              | Individuals and Societies (12 Units)  
|                              | Diversity Requirement  
| Pre-major? (Yes/No. If yes, provide requirements). Provide email(s)/letter(s) of support from home department head(s) for courses not owned by your department. | No  
| List any special requirements to declare or gain admission to this major (completion of specific coursework, minimum GPA, interview, application, etc.) | The Cyber Operations program requires a supplemental program application in addition to admission to The University of Arizona. The entrance requirements include:  
• Minimum 2.5 GPA in your college coursework  
• Resume  
• Goal statement  
Cyber Engineering Subplan:  
• AAS degree in computer science related field (recommended)  
• ECE 175: Computer Programming for Engineering Applications (3 units)  
• BASV 300, MATH 243 or CSC 245: Intro to Discrete Math (3 units)  
Defense/Forensics and Cyber Law and Policies Subplans:  
• AAS degree in Cybersecurity related field (recommended)  
| Major requirements |  
| Minimum # of units required in major (units counting towards major units and major GPA) | 42 Units  
| Minimum # of upper-division units required in the major (upper division units counting towards major GPA) | 39 Units  
| Minimum # of residency units to be completed in the major | 30 Units  
| Required supporting coursework (courses that do not count towards major units and major GPA, but are required for the major) | N/A |
Courses listed must include subject code, units, and title. 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.

<table>
<thead>
<tr>
<th>Major requirements (list all required major coursework including major core, major electives, sub-plan core, and sub-plan electives; courses count towards major units and major GPA) 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.</th>
<th>BAS in Cyber Operations Core (27 units)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 301: Fundamentals Cybersecurity (3 units)</td>
<td>CYBV 301: Fundamentals Cybersecurity (3 units)</td>
</tr>
<tr>
<td>ENGV 306: Advanced Composition (3 units)</td>
<td>ENGV 306: Advanced Composition (3 units)</td>
</tr>
<tr>
<td>INFV 320: Computational Thinking and Doing (3 units)</td>
<td>INFV 320: Computational Thinking and Doing (3 units)</td>
</tr>
<tr>
<td>BASV 314: Mathematics for Applied Science (3 units) -or- BASV 376: Mathematics for Applied Technology (3 units)</td>
<td>BASV 314: Mathematics for Applied Science (3 units) -or- BASV 376: Mathematics for Applied Technology (3 units)</td>
</tr>
<tr>
<td>CYBV326: Intro Methods of Network Analysis (3 units)</td>
<td>CYBV326: Intro Methods of Network Analysis (3 units)</td>
</tr>
<tr>
<td>CYBV329: Cyber Ethics (3 units)</td>
<td>CYBV329: Cyber Ethics (3 units)</td>
</tr>
<tr>
<td>CYBV 385: Intro to Cyber Operations (3 units)</td>
<td>CYBV 385: Intro to Cyber Operations (3 units)</td>
</tr>
<tr>
<td>CYBV 400: Active Cyber Defense (3 units)</td>
<td>CYBV 400: Active Cyber Defense (3 units)</td>
</tr>
<tr>
<td>CYBV 498: Senior Capstone (3 units)</td>
<td>CYBV 498: Senior Capstone (3 units)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Engineering Subplan Core (15 units)</th>
<th>CYBV 470: C Programming for Security Professionals (3 units) or CSCV 352: System Programming &amp; Unix (3 units)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 454: Malware Threats &amp; Analysis (3 units)</td>
<td>CYBV 454: Malware Threats &amp; Analysis (3 units)</td>
</tr>
<tr>
<td>CYBV 471: Assembly Language (3 units)</td>
<td>CYBV 471: Assembly Language (3 units)</td>
</tr>
<tr>
<td>CYBV 479: Wireless Network &amp; Security (3 units)</td>
<td>CYBV 479: Wireless Network &amp; Security (3 units)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defense/Forensics Subplan Core (15 units)</th>
<th>CYBV 388: Cyber Investigations &amp; Forensics (3 units)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 435: Cyber Threat Intelligence (3 units)</td>
<td>CYBV 435: Cyber Threat Intelligence (3 units)</td>
</tr>
<tr>
<td>CYBV 454: Malware Threats &amp; Analysis (3 units)</td>
<td>CYBV 454: Malware Threats &amp; Analysis (3 units)</td>
</tr>
<tr>
<td>CYBV 480: Cyber Warfare (3 units)</td>
<td>CYBV 480: Cyber Warfare (3 units)</td>
</tr>
</tbody>
</table>

**Choose 1**
- CYBV 436: Counter Cyber Threat Intelligence (3 units)
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 473</td>
<td>Violent Python (3 units)</td>
</tr>
<tr>
<td>CYBV 477</td>
<td>Advanced Computer Forensics (3 units)</td>
</tr>
<tr>
<td>CYBV 481</td>
<td>Social Engineering Attacks &amp; Defenses (3 units)</td>
</tr>
</tbody>
</table>

**Cyber Law and Policy Subplan Core (15 units)**

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPSV 314</td>
<td>National Security Policy (3 units)</td>
</tr>
<tr>
<td>GPSV 461</td>
<td>Civil Liberties and the U.S. Constitution (3 units)</td>
</tr>
<tr>
<td>CYBV 435</td>
<td>Cyber Threat Intelligence (3 units)</td>
</tr>
</tbody>
</table>

**Choose 2**

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 436</td>
<td>Counter Cyber Threat Intelligence (3 units)</td>
</tr>
<tr>
<td>GPSV 441</td>
<td>American Foreign Policy (3 units)</td>
</tr>
<tr>
<td>GPSV 442</td>
<td>International Law (3 units)</td>
</tr>
<tr>
<td>GPSV 471</td>
<td>National Security &amp; Intelligence (3 units)</td>
</tr>
<tr>
<td>GPSV 473</td>
<td>National Security Operations &amp; Issues (3 units)</td>
</tr>
<tr>
<td>CYBV 473</td>
<td>Violent Python (3 units)</td>
</tr>
<tr>
<td>GPSV 474</td>
<td>Politics of Terrorism (3 units)</td>
</tr>
<tr>
<td>GPSV 496</td>
<td>Special Topics in Regional Politics and Security (3 units)</td>
</tr>
</tbody>
</table>

**Internship, practicum, applied course requirements (Yes/No. If yes, provide description)**

Yes. Students must complete CYBV498, Senior Capstone, with a minimum 45 hour student engagement experience.

**Senior thesis or senior project required (Yes/No. If yes, provide description)**

Yes. Students engage in a senior project and write a senior project thesis paper as part of the CYBV498—Senior Capstone.

**Additional requirements (provide description)**

Students must earn a minimum 2.0 major GPA.

**Students in the Cyber Engineering subplan must complete the Cyber Operations Undergraduate Certificate. In addition to the subplan requirements, the following courses are required for the Cyber Operations Undergraduate Certificate:**

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV472</td>
<td>Secure Software Development &amp; Assessment (3 units)</td>
</tr>
<tr>
<td>CYBV389</td>
<td>Operating System Theory for Security Professionals (3 units) or CSCV452 Principles of Operating Systems (4 units)</td>
</tr>
<tr>
<td>NETV379</td>
<td>Cloud Computing (3 units)</td>
</tr>
</tbody>
</table>

**Minor (specify if optional or required)**

Optional

**Any double-dipping restrictions? (Yes/No. If yes, provide description)**

No
III. **CURRENT COURSES**—using the table below, list existing courses included in the proposed major. 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 program 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. Add rows to the table, as needed.

<table>
<thead>
<tr>
<th>Course prefix and number (include cross-listings)</th>
<th>Units</th>
<th>Title</th>
<th>Course Description</th>
<th>Pre-requisites</th>
<th>Modes of delivery (online, in-person, hybrid)</th>
<th>Typically Offered (F, W, Sp, Su)</th>
<th>Dept signed party to proposal? (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV301</td>
<td>3</td>
<td>Fundamentals of Cybersecurity</td>
<td>CYBV 301 will provide students with an introduction to Fundamentals of Cybersecurity, which will include an introduction to cyber security policy, doctrine, and operational constraints. A broad survey of cybersecurity concepts, tools, technologies and best practices will be presented. Students will use hands-on activities to become familiar with and practice cybersecurity techniques and procedures.</td>
<td>None</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp, Su</td>
<td>Yes</td>
</tr>
<tr>
<td>CYBV326</td>
<td>3</td>
<td>Introductory Methods of Network Analysis</td>
<td>Provides a methodology for analyzing networks by examining the network at its infrastructure, network and applications layers; exploring how they transfer data; investigating how network protocols work to enable</td>
<td>None</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp, Su</td>
<td>Yes</td>
</tr>
</tbody>
</table>
communication; and probing and analyzing how the lower-level network layers support the upper ones. Students will use hands-on labs and exercises to investigate and analyze network fundamentals.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Units</th>
<th>Course Title</th>
<th>Description</th>
<th>Designation</th>
<th>Delivery</th>
<th>Terms</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV329</td>
<td>3</td>
<td>Cyber Law, Ethics &amp; Policy</td>
<td>A sustained study of ethical issues that arise in relation to employment in the public and private sectors, including allocation of resources, corporate and social responsibility, relationships, and discrimination. This course is a designated writing emphasis course. A main focus of this course will be on the ethical and legal standards governing information technology. New technology creates ethical challenges for individuals around the globe, and applies to most persons regardless of whether they are employed in the information technology field or a more traditional occupation.</td>
<td>None</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp, Su</td>
<td>CYBV301 or Requirement Designation CYBR or Consent of Instructor</td>
</tr>
<tr>
<td>CYBV385</td>
<td>3</td>
<td>Introduction to Cyber Operations</td>
<td>An introduction to the concepts of cyber operations, applying fundamentals of network operations to understanding network attack and defense concepts. Students will recognize common cyber-attacks and the techniques for identifying, detecting and defending against</td>
<td>CYBV301 or Requirement Designation CYBR or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp, Su</td>
<td>Yes</td>
</tr>
</tbody>
</table>
cyber security threats. Students will learn the basics of physical, network and web security as well as standards and laws in cyber security. Legal, ethical, and privacy issues will be discussed. Students will use hands-on labs and exercises to illustrate the workings of information security technologies.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Credits</th>
<th>Course Title</th>
<th>Description</th>
<th>Prerequisites</th>
<th>Delivery Options</th>
<th>Offered Terms</th>
<th>Corequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV388</td>
<td>3</td>
<td>Cyber Investigations and Forensics</td>
<td>Study of intrusion detection methodologies, tools, and approaches to incident response; examination of computer forensic principles, including operating system concepts, registry structures, file system concepts, boot process, low level hardware calls, and file operations; and an exploration of the ethical and legal issues attendant to cyber investigations and forensics.</td>
<td>INFV320 and CYBV 385 or NETV 385 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>CYBV389</td>
<td>3</td>
<td>Operating System Theory for Security Professionals</td>
<td>Provides students a thorough understanding of operating systems theory and implementation. They will be able to understand operating system internals to the level that they could design and implement significant architectural changes to an existing OS.</td>
<td>INFV320 and CSCV352 or consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>CYBV400</td>
<td>3</td>
<td>Active Cyber Defense</td>
<td>Provides students with an introduction to the policies,</td>
<td>INFV 320 and CYBV 385 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
<td>Yes</td>
</tr>
</tbody>
</table>
techniques, and operational capabilities and limitations of implementing an Active Cyber Defense program. A broad survey of development of defensible network architectures; integration of passive defensive technologies; consumption and production of Cyber Threat Intelligence (CTI) products; implementation of Network Security Monitoring (NSM) and Hunt Teaming (HT) operations; employment of Incident Response (IR) plans; and Threat and Environment Manipulation techniques (TEM) will be presented, and students will use hands-on activities to practice and implement active defense methodologies.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Credits</th>
<th>Title</th>
<th>Description</th>
<th>Prerequisites</th>
<th>Delivery</th>
<th>Offered</th>
<th>Satisfies Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV435</td>
<td>3</td>
<td>Cyber Threat Intelligence</td>
<td>An investigation of threat actors and the techniques they employ to attack networks. Students will research threat capabilities and objectives. Formal ethical hacking methodology including reconnaissance, scanning and enumeration, gaining access, escalation of privilege, maintain access and reporting is examined.</td>
<td>INFV 320 and CYBV 385 or consent of instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>CYBV436</td>
<td>3</td>
<td>Counter Cyber Threat Intelligence</td>
<td>CYBV 436 will provide students with an in-depth examination of the tactics, techniques, and</td>
<td>CYBV435 or consent of instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
<td>Yes</td>
</tr>
</tbody>
</table>
procedures used to conduct online anonymization and attribution. An extensive analysis of the concepts, technologies, and best practices will be presented. Students will use interactive activities to become familiar with and practice the protection of their online identity.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Units</th>
<th>Course Title</th>
<th>Description</th>
<th>Prerequisites</th>
<th>Schedule</th>
<th>Offered</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV454</td>
<td>3</td>
<td>Malware Threats &amp; Analysis</td>
<td>Provides students a methodology to perform safely static and dynamic analysis of software of potentially unknown origin, including obfuscated malware, and to understand fully the software's functionality and specifications. Students will use hands-on labs and exercises to examine the fundamental principles of malware analysis and software reverse engineering.</td>
<td>INFV 320 or consent of instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
</tr>
<tr>
<td>CYBV470</td>
<td>3</td>
<td>C Programming for Security Professionals</td>
<td>Provides students with an introduction to C programming. Students will use hands-on labs and exercises to practice and implement applications developed in the C programming language.</td>
<td>INFV 320 or consent of instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
</tr>
<tr>
<td>CYBV471</td>
<td>3</td>
<td>Assembly Language Programming for Security Professionals</td>
<td>Will provide students with an introduction to assembly language programming. Students will use hands-on labs and exercises to practice and implement applications developed in Assembly language.</td>
<td>Prerequisites INFV 320 and CYBV 470</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
</tr>
<tr>
<td>Course Code</td>
<td>Units</td>
<td>Course Title</td>
<td>Description</td>
<td>Prerequisites</td>
<td>Delivery</td>
<td>Offered Terms</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>CYBV472</td>
<td>3</td>
<td>Secure Software Development &amp; Assessment</td>
<td>Provides students with an introduction to the secure software development process as well as how to conduct a software security analysis to detect the presence of weaknesses that may lead to exploitable vulnerabilities in operational systems. Students will learn how to write, analyze, and test secure software that maintains Confidentiality, Integrity and Availability.</td>
<td>INFV 320 and CYBV 454, 470 &amp; 471 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
</tr>
<tr>
<td>CYBV473</td>
<td>3</td>
<td>Violent Python</td>
<td>CYBV 473 will provide students with advanced practical applications of Python programming to support offensive and defensive cybersecurity operations. A crosscut of Python concepts, tools, and techniques will be presented. Students will use interactive programming activities to master and create advanced Python tools to support common cybersecurity tasks.</td>
<td>INFV 320 or consent of instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp, Su</td>
</tr>
<tr>
<td>CYBV477</td>
<td>3</td>
<td>Advanced Computer Forensics</td>
<td>An advanced forensics course that provides students an in-depth knowledge of network forensics, network flow analysis, network intrusion detection systems, event reconstruction and memory forensics for Windows, Linux and MAC operating systems.</td>
<td>INFV 320 and CYBV 388 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F</td>
</tr>
<tr>
<td>Course Code</td>
<td>Credits</td>
<td>Course Title</td>
<td>Description</td>
<td>Prerequisites</td>
<td>Delivery</td>
<td>Semester</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>------------------</td>
<td>----------</td>
</tr>
<tr>
<td>CYBV479</td>
<td>3</td>
<td>Wireless Networking and Security</td>
<td>Provides an introduction to wireless networking, mobile device hardware and software architectures as well as the application of security fundamentals for mobile computing systems. Students will be able to describe user associations and routing in a cellular/mobile network, interaction of elements within the cellular/mobile core, and end-to-end delivery of a packet and/or signal and what happens with the hand-off at each step along the communications path. They will be able to explain differences in core architecture between different generations of cellular and mobile network technologies.</td>
<td>CYBV326 and CYBV385 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
</tr>
<tr>
<td>CYBV480</td>
<td>3</td>
<td>Cyber Warfare</td>
<td>Provides an introduction to cyber warfare along with its policy, doctrine, and operational constraints. A broad survey of cyber tools, techniques and procedures will be presented, and students will use hands-on labs to practice and implement attack and defense methodologies.</td>
<td>INFV320 and CYBV385 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
</tr>
<tr>
<td>CYBV481</td>
<td>3</td>
<td>Social Engineering Attacks and Defenses</td>
<td>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</td>
<td>CYBV 480 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
</tr>
</tbody>
</table>
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 master social engineering attacks and defenses in order to be able to develop policies and procedures to increase organizational security posture.

**CYBV498**

3 Capstone in Cyber Operations

A culminating experience for majors involving a substantive project that includes an engagement experience and demonstrates a synthesis of learning accumulated in the major, including broadly comprehensive knowledge of the discipline and its methodologies. Senior standing required.

**CSCV352**

3 System Programming and Unix

Programming in C, including single and multi-dimensional arrays, lists, stacks, queues, trees, and bit manipulation. Unix topics, including debuggers, makefiles, shell programming, and other topics that support systems programming.

Prerequisite or concurrent registration, CSC 252 or Consent of Instructor.

**CSCV452**

4 Principles of Operating Systems

Concepts of modern operating systems; concurrent processes; process synchronization and communication; resource allocation; kernels; deadlock;

CSCV 352 or CSC 352
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Credits</th>
<th>Course Title</th>
<th>Description</th>
<th>Prerequisites</th>
<th>Delivery</th>
<th>Offered Terms</th>
<th>Instructor Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENGV306</td>
<td>3</td>
<td>Advanced Composition</td>
<td>Study of genre and rhetorical situation; advanced practice in expository writing.</td>
<td>ENGL 102</td>
<td>Online, In-person, Hybrid</td>
<td>F</td>
<td>Yes</td>
</tr>
<tr>
<td>INVF320</td>
<td>3</td>
<td>Computational Thinking and Doing</td>
<td>This course provides an overview of basics of programming and techniques used by computing professionals in a variety of application areas. Topics include computation, programs, algorithms, programming languages, and complexity, as well as how these concepts and techniques are used to solve problems in Informatics.</td>
<td>None</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>BASV314</td>
<td>3</td>
<td>Mathematics for Applied Science</td>
<td>This course will examine applications of probability, statistics, data analysis, hypothesis testing, apportionment and scheduling to the applied sciences. Registration requires a passing grade on the UA South BAS Math Readiness test.</td>
<td>Students must be admitted to the UA South BAS Program or consent of instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F, Sp, Su</td>
<td>Yes</td>
</tr>
<tr>
<td>BASV376</td>
<td>3</td>
<td>Mathematics for Applied Technology</td>
<td>Basic probability inc. permutations, combinations, and counting theory; number systems: binary and hexadecimal; converting between number bases; solving application problems; using Excel with statistical functions.</td>
<td>Prerequisites BASV 300, MATH 243, or CSC 245</td>
<td>Online, In-person, Hybrid</td>
<td>F</td>
<td>Yes</td>
</tr>
<tr>
<td>GPSV314</td>
<td>3</td>
<td>National Security Policy</td>
<td>Decision-making structures, processes, and outcomes relevant to American security policy;</td>
<td>POL 201 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>Course Code</td>
<td>Credits</td>
<td>Course Title</td>
<td>Description</td>
<td>Prerequisites</td>
<td>Delivery Method</td>
<td>Grade</td>
<td>Mix</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>GPSV441</td>
<td>3</td>
<td>American Foreign Policy</td>
<td>Analysis of American Foreign Policy from the Cold War to the present; Congressional-Executive clashes over foreign policy control; approaches to policy analysis. This is a writing emphasis course.</td>
<td>GPSV 301 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>F</td>
<td>Yes</td>
</tr>
<tr>
<td>GPSV442</td>
<td>3</td>
<td>International Law</td>
<td>The international state system; legal-political problems, including territory, environment, seas.</td>
<td>POL 202 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>GPSV461</td>
<td>3</td>
<td>Civil Liberties and the U.S. Constitution</td>
<td>Analysis of the constitutional guarantees of civil liberties in the U.S. Constitution.</td>
<td>GPSV 301 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>GPSV471</td>
<td>3</td>
<td>National Security and Intelligence</td>
<td>Overview of the role of intelligence in the formulation and execution of US national security policy. Will include a detailed look at challenges facing both the analysis of intelligence information and the introduction of that analysis into the national security policy process. Will also entail close reading and discussion of selected declassified intelligence documents.</td>
<td>None</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>GPSV473</td>
<td>3</td>
<td>National Security Operations &amp; Issues</td>
<td>This course is intended to familiarize students with the basic purposes and nature of US covert action and to help them understand its historical development. More fundamentally, the course will seek</td>
<td>GPSV 301 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
</tbody>
</table>
to illustrate both covert actions' potential utility and its inherent limitations and challenges; challenges that in some respects have intensified with the rise of non-state actors, the information revolution, and other aspects of the post-Cold War environment. Finally, the course will draw implications for the role of covert action against current national security challenges, especially global terror networks.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Credits</th>
<th>Course Title</th>
<th>Description</th>
<th>Prerequisites</th>
<th>Mode</th>
<th>Term</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPSV474</td>
<td>3</td>
<td>Politics of Terrorism</td>
<td>An introduction to theories of international relations as applied to the study of terrorism, including an examination of major discourses on the conduct of state systems, the foundations of modern terrorism and associated evolution of ideology, tactics, and strategies; and evaluation of terrorist ideologies and how that evaluation can develop a framework for critical analysis.</td>
<td>GPSV 301 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>GPSV496</td>
<td>3</td>
<td>Special Topics in Regional Politics and Security</td>
<td>Survey and analysis of the leading political and economic issues of interest in various world regions. Specific regions and topics will depend on student need and interest, and the research/teaching interests of the participating faculty member.</td>
<td>GPSV 301 or Consent of Instructor</td>
<td>Online, In-person, Hybrid</td>
<td>Sp</td>
<td>Yes</td>
</tr>
<tr>
<td>NETV379</td>
<td>3</td>
<td>Cloud Computing</td>
<td>Course covers the theory and application of cloud computing, including Cloud Computing network design and connectivity, server management, best-practices, security, and provider service level agreements. Case studies of industry examples are used as applications to reinforce the discussed theories.</td>
<td>None</td>
<td>Online, In-person, Hybrid</td>
<td>F, Su</td>
<td>Yes</td>
</tr>
</tbody>
</table>
IV. **NEW COURSES NEEDED** – using the table below, list any new courses that must be created to initiate the major. If 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.

<table>
<thead>
<tr>
<th>Course prefix and number (include cross-listings)</th>
<th>Units</th>
<th>Title</th>
<th>Course Description</th>
<th>Pre-requisites</th>
<th>Modes of delivery (online, in-person, hybrid)</th>
<th>Status*</th>
<th>Anticipated first term offered</th>
<th>Typically Offered (F, W, Sp, Su)</th>
<th>Dept signed party to proposal? (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*In development (D); submitted for approval (S); approved (A)

Subject description for new prefix (if requested). Include your requested prefix, if any. : N/A
**FOUR-YEAR PLAN** – provide a sample four-year degree plan that includes all requirements to graduate with this major and takes into consideration course offerings and sequencing. Refer to Degree Search for examples. Use generic title/placeholders for requirements with more than one course option (e.g. Upper Division Major Elective, Minor Course, Second Language, GE Tier 1, GE Tier 2). Add rows as needed.

### Cyber Engineering SubPlan & Required Cyber Operations Undergraduate Certificate

<table>
<thead>
<tr>
<th>Semester 1</th>
<th>Semester 2</th>
<th>Semester 3</th>
<th>Semester 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course prefix and number</td>
<td>Units</td>
<td>Course prefix and number</td>
<td>Units</td>
</tr>
<tr>
<td>ENGL 101</td>
<td>3</td>
<td>ENGL 102</td>
<td>3</td>
</tr>
<tr>
<td>Associates Required Math Course</td>
<td>3</td>
<td>2nd Semester Second Language</td>
<td>4</td>
</tr>
<tr>
<td>Additional Transfer Coursework from Associate's Degree</td>
<td>9</td>
<td>Additional Transfer Coursework from Associate's Degree</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Semester 5</th>
<th>Semester 6</th>
<th>Semester 7</th>
<th>Semester 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course prefix and number</td>
<td>Units</td>
<td>Course prefix and number</td>
<td>Units</td>
</tr>
<tr>
<td>CYBV 301: Fundamentals of Cybersecurity</td>
<td>3</td>
<td>CYBV 326: Network Analysis</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
</tr>
<tr>
<td>Course</td>
<td>Credits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 385: Intro to Cyber Operations</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 329: Cyber Ethics</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 480: Cyber Warfare</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 472: Secure Software Design and Analysis (Required for the Cyber Operations Certificate)</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFV 320: Computational Thinking &amp; Doing</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 471: Assembly Language Programming for Security Professionals</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 479: Wireless Networking</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETV 379: Cloud Computing (Required for the Cyber Operations Certificate)</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BASV 376: Mathematics for Applied Technology</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier II Individuals &amp; Societies</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier II Natural Sciences</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier II Arts/Humanities</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier II Arts/Humanities</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier II Individuals &amp; Societies</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>18</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Defense & Forensics SubPlan

<table>
<thead>
<tr>
<th>Semester 1</th>
<th>Semester 2</th>
<th>Semester 3</th>
<th>Semester 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course prefix and number</td>
<td>Units</td>
<td>Course prefix and number</td>
<td>Units</td>
</tr>
<tr>
<td>ENGL 101</td>
<td>3</td>
<td>ENGL 102</td>
<td>3</td>
</tr>
<tr>
<td>Associates Required Math Course</td>
<td>3</td>
<td>2nd Semester Second Language</td>
<td>4</td>
</tr>
<tr>
<td>Additional Transfer Coursework from Associate's Degree</td>
<td>9</td>
<td>Additional Transfer Coursework from Associate's Degree</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>15</td>
<td><strong>Total</strong></td>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Semester 5</th>
<th>Semester 6</th>
<th>Semester 7</th>
<th>Semester 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course prefix and number</td>
<td>Units</td>
<td>Course prefix and number</td>
<td>Units</td>
</tr>
<tr>
<td>CYBV 301: Fundamentals of Cybersecurity</td>
<td>3</td>
<td>CYBV 388: Cyber Forensics &amp; Investigations</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 326: Network Analysis</td>
<td>3</td>
<td>CYBV 400: Active Cyber Defense</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 385: Intro to Cyber Operations</td>
<td>3</td>
<td>CYBV 480: Cyber Warfare</td>
<td>3</td>
</tr>
</tbody>
</table>
### Cyber Law & Policy SubPlan

<table>
<thead>
<tr>
<th>Semester 1</th>
<th>Semester 2</th>
<th>Semester 3</th>
<th>Semester 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course prefix and number</strong></td>
<td><strong>Units</strong></td>
<td><strong>Course prefix and number</strong></td>
<td><strong>Units</strong></td>
</tr>
<tr>
<td>ENGL 101</td>
<td>3</td>
<td>ENGL 102</td>
<td>3</td>
</tr>
<tr>
<td>Tier II Arts/Humanities</td>
<td>3</td>
<td>Tier II Individuals &amp; Societies</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>15</td>
<td><strong>Total</strong></td>
<td>15</td>
</tr>
</tbody>
</table>

### Semester 5

<table>
<thead>
<tr>
<th><strong>Course prefix and number</strong></th>
<th><strong>Units</strong></th>
<th><strong>Course prefix and number</strong></th>
<th><strong>Units</strong></th>
<th><strong>Course prefix and number</strong></th>
<th><strong>Units</strong></th>
<th><strong>Course prefix and number</strong></th>
<th><strong>Units</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 301: Fundamentals of Cybersecurity</td>
<td>3</td>
<td>INFV 320: Computational Thinking &amp; Doing</td>
<td>3</td>
<td>BASV 314: Mathematics for Applied Sciences</td>
<td>3</td>
<td>CYBV 498: Senior Capstone</td>
<td>3</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Credits</td>
<td>Course Code</td>
<td>Course Title</td>
<td>Credits</td>
<td>Course Code</td>
<td>Course Title</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------</td>
<td>---------</td>
<td>-------------</td>
<td>--------------------------------------------------</td>
<td>---------</td>
<td>-------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ENGV 306:</td>
<td>Advanced Composition</td>
<td>3</td>
<td>CYBV 435:</td>
<td>Cyber Threat Intelligence</td>
<td>3</td>
<td>Cyber Law &amp; Policy Elective</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 385:</td>
<td>Intro to Cyber Operations</td>
<td>3</td>
<td>GPSV 61:</td>
<td>Civil Liberties &amp; US Constitution</td>
<td>3</td>
<td>CYBV 400:</td>
<td>Active Cyber Defense</td>
</tr>
<tr>
<td>GPSV 314:</td>
<td>National Security Policy</td>
<td>3</td>
<td>CYBV 326:</td>
<td>Network Analysis</td>
<td>3</td>
<td>Tier II</td>
<td>Natural Sciences</td>
</tr>
<tr>
<td>Tier II</td>
<td>Arts/Humanities</td>
<td>3</td>
<td>Tier II</td>
<td>Individuals &amp; Societies</td>
<td>3</td>
<td>Tier II</td>
<td>Individuals &amp; Societies</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>15</td>
<td>Total</td>
<td></td>
<td>15</td>
<td>Total</td>
<td></td>
</tr>
</tbody>
</table>
V. **STUDENT LEARNING OUTCOMES AND CURRICULUM MAP**—describe what students should know, understand, and/or be able to do at the conclusion of this major. Work with [Office of Instruction and Assessment](#) to create a curricular map using Taskstream. Include your curricular map in this section (refer to Appendix C for sample Curriculum Map).

| Operating Systems & Low Level Programming | Demonstrate a thorough understanding of various operating systems and be able to develop low level applications with the required complexity and sophistication to implement exploits for discovered vulnerabilities. |
| Malware Reverse Engineering | Safely perform static and dynamic analysis of unknown software, including obfuscated malware, to fully understand the software’s functionality. |
| Offensive Cyber Operations | Explain and demonstrate the phases of offensive cyber operations; what each phase entails; who has the authorities to conduct each phase; and how operations are assessed after completion. |
| Defensive Cyber Operations | Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals. |
| Forensics | Demonstrate and explain how to acquire a forensically sound image; understand user activity; determine the manner in which an operating system or application has been subverted; identify forensic artifacts left by attacks; and recover deleted and/or intentionally hidden information. |
| Networking | Demonstrate a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones. |
| Critical Thinking & Problem Solving | Demonstrate understanding of how variability affects outcomes; how to identify anomalous events; how to integrate and differentiate continuous functions of multiple variables; and how to solve complex problems using computation and scripting languages. |
| Law, Ethics, & Policy | Describe and explain the relationship between cyber ethics and law; US and International cyber laws; criminal penalties related to unethical hacking; and apply the notion of Gray Areas to articulate where the law has not yet caught up to technology innovation. |
| **Security Principles & Vulnerabilities** | Demonstrate and explain the various types of vulnerabilities and their underlying causes; how security principles interrelate and are typically employed to achieve assured solutions; and explain how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation. |
| **Cyber Threat Intelligence** | Describe and demonstrate how knowledge about an adversary's motivation, intentions, and methods are collected, analyzed, and disseminated to help security personnel and business staff to align resources and protect critical assets within an enterprise architecture. |
## Curriculum Map:

### BAS in Cyber Operations

**Courses and Activities Mapped to Cyber Operations Outcome Set**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>I</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>I</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

### Courses and Learning Activities

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Hours</th>
<th>Introduce</th>
<th>Practice</th>
<th>Assessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV201</td>
<td>Fundamentals of Cybersecurity</td>
<td></td>
<td>I</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>INPV330</td>
<td>Computational Thinking &amp; Doing</td>
<td></td>
<td>I</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV636</td>
<td>Introductory Methods of Network Analysis</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV529</td>
<td>Cyber Law, Ethics &amp; Policy</td>
<td></td>
<td>I</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV555</td>
<td>Introduction to Cyber Operations</td>
<td></td>
<td>I</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV598</td>
<td>Operating System Theory for Security Professionals</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV405</td>
<td>Active Cyber Defense</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV560</td>
<td>Cyber Threat Intelligence</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV101</td>
<td>Malware Threats and Analysis</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV470</td>
<td>Assembly Language Programming for Security Professionals</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV605</td>
<td>Wireless Networking &amp; Security</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV410</td>
<td>Cyber Warfare</td>
<td></td>
<td>P</td>
<td>P</td>
<td>A</td>
</tr>
<tr>
<td>CYBV230</td>
<td>Digital Forensics in Cyber Operations</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

**Legend:**
- I: Introduced
- P: Practiced
- A: Assessed

**Last Modified:** 11/16/2018 03:35:32 PM

VI. **ASSESSMENT PLAN FOR STUDENT LEARNING** - using the table below, provide a schedule for program assessment of intended student learning outcomes 1) while students are in the program and 2) after completion of the major. Add rows as needed. Delete **EXAMPLE** row.

<table>
<thead>
<tr>
<th>Learning Outcomes</th>
<th>Sources(s) of Evidence</th>
<th>Assessment Measures</th>
<th>Data Collection Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outcome 1: Demonstrate a thorough understanding of various operating systems and be able to develop low level applications with the required complexity and sophistication to implement exploits for discovered vulnerabilities.</td>
<td>Course-embedded assessments</td>
<td>Exams &amp; coding assignments</td>
<td>End of CYBV389&lt;br&gt;End of CYBV454&lt;br&gt;End of CYBV471&lt;br&gt;End of CYBV498</td>
</tr>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td></td>
<td>See attached sample surveys in Appendices E &amp; F</td>
<td></td>
<td>End of CYBV498</td>
</tr>
<tr>
<td>Outcome 2: Safely perform static and dynamic analysis of unknown software, including obfuscated malware, to fully understand the software's functionality.</td>
<td>Course-embedded assessments</td>
<td>Exams, practical exercises, &amp; reports</td>
<td>End of CYBV385&lt;br&gt;End of CYBV454</td>
</tr>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td></td>
<td>See attached sample surveys in Appendices E &amp; F</td>
<td></td>
<td>End of CYBV498</td>
</tr>
<tr>
<td>Outcome 3: Explain and demonstrate the phases of offensive cyber operations; what each phase entails; who has the authorities to conduct each phase; and how operations are assessed after completion.</td>
<td>Course-embedded assessments</td>
<td>Exams, practical exercises, &amp; reports</td>
<td>End of CYBV301&lt;br&gt;End of CYBV326&lt;br&gt;End of CYBV329&lt;br&gt;End of CYBV385&lt;br&gt;End of CYBV400&lt;br&gt;End of CYBV435&lt;br&gt;End of CYBV479&lt;br&gt;End of CYBV480</td>
</tr>
<tr>
<td>Outcome 4: Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.</td>
<td>Course-embedded assessments</td>
<td>Exams, practical exercises, &amp; reports</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See attached sample surveys in Appendices E &amp; F</td>
<td>End of CYBV498</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outcome 5: Demonstrate and explain how to acquire a forensically sound image; understand user activity; determine the manner in which an operating system or application has been subverted; identify forensic artifacts left by attacks; and recover deleted and/or intentionally hidden information.</th>
<th>Course-embedded assessments</th>
<th>Exams, practical exercises, &amp; reports</th>
<th>End of CYBV498</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See attached sample surveys in Appendices E &amp; F</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td>Outcome 6: Demonstrate a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones.</td>
<td>Course-embedded assessments</td>
<td>Exams, practical exercises, &amp; reports</td>
<td>End of CYBV301 End of CYBV326 End of CYBV479</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See attached sample surveys in Appendices E &amp; F</td>
<td>End of CYBV498</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outcome 7: Demonstrate understanding of how variability affects outcomes; how to identify anomalous events; how to integrate and differentiate continuous functions of multiple variables; and how to solve complex problems using computation and scripting languages.</th>
<th>Course-embedded assessments</th>
<th>Exams, homework assignments &amp; coding assignments</th>
<th>End of CYBV301 End of INFV320 End of CYBV329 End of CYBV435</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See attached sample surveys in Appendices E &amp; F</td>
<td>End of CYBV498</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outcome 8: Describe and explain the relationship between cyber ethics and law; US and International cyber laws; criminal penalties related to unethical hacking; and apply the notion of Gray Areas to articulate where the law has</th>
<th>Course-embedded assessments</th>
<th>Exams &amp; case study papers</th>
<th>End of CYBV301 End of CYBV329 End of CYBV400 End of CYBV480</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Comprehensive research project and report</td>
<td>End of CYBV498</td>
</tr>
<tr>
<td>Outcome 9: Demonstrate and explain the various types of vulnerabilities and their underlying causes; how security principles interrelate and are typically employed to achieve assured solutions; and explain how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.</td>
<td>Course-embedded assessments</td>
<td>Exams, practical exercises, &amp; reports</td>
<td>Comprehensive research project and report</td>
</tr>
<tr>
<td>Outcome 10: Describe and demonstrate how knowledge about an adversary's motivation, intentions, and methods are collected, analyzed, and disseminated to help security personnel and business staff to align resources and protect critical assets within an enterprise architecture.</td>
<td>Course-embedded assessments</td>
<td>Exams, practical exercises, &amp; reports</td>
<td>Comprehensive research project and report</td>
</tr>
<tr>
<td></td>
<td>Student learning &amp; program assessment surveys</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VII. **PROGRAM ASSESSMENT PLAN** - using the table below, provide a schedule for program evaluation 1) while students are in the program and 2) after completion of the major. Add rows as needed. Delete **EXAMPLE** rows.

<table>
<thead>
<tr>
<th>Assessment Measure</th>
<th>Source(s) of Evidence</th>
<th>Data Collection Point(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Placement Statistics</td>
<td>Student/Alumni Survey</td>
<td>At graduation and as part of alumni survey</td>
</tr>
<tr>
<td>Academic Program Review</td>
<td>Reviewers’ responses</td>
<td>Every 7 years</td>
</tr>
<tr>
<td>Program Curriculum Review</td>
<td>Interdisciplinary Board reviewer’s response</td>
<td>Biannually</td>
</tr>
<tr>
<td>Advisory Board Program Review</td>
<td>Advisory Board reviewer’s response</td>
<td>Biannually</td>
</tr>
<tr>
<td>NSA CAE-CO Designation Renewal</td>
<td>NSA reviewer responses</td>
<td>Every 5 years</td>
</tr>
</tbody>
</table>

To provide information to the Program Director, faculty members, and Advisory Board, the Cyber Operations Program Office will administer surveys to the graduates of the Cyber Operations degree program. The first survey will be administered in the CYBV 498 program capstone course, and will be a required course component. A draft of this survey instrument is included, and is designed to provide more general information about student opinions on the degree program’s alumni support options, job placement, and preparedness to work in the Cyber Operations field. Subsequently, this survey will be emailed out by the Program Manager for Cyber Operations three months after graduation, with a telephone call reminder to complete the survey from the Cyber Operations Program Office. It will be emailed out again nine months after graduation, with a reminder call if necessary, from the Cyber Operations Program Office. Thereafter, the survey will be administered once per year to continue to provide longitudinal data to the Program Director, faculty members, and the Advisory Board.

Further program assessment will be provided by the Advisory Board. To meet the needs for being recognized as a Servicemembers Opportunity College for Cyber Operations, the Cyber Operations program needed to create an Advisory Board to provide input to the Program Director and faculty on changing industry needs and developments that may need to be included in the current course curriculum. The Advisory Board consists of leaders in different portions of the cyber field, including those working in the government, the military, and private sector. The Advisory Board will be convened twice each calendar year for a meeting with the current faculty members and the Program Director to review the Cyber Operations BAS curriculum to be certain it is adjusting as needed to meet market demands and to ensure that the knowledge, skills, and abilities employers are seeking are being addressed by our curriculum.
As part of the NSA designation process, the Cyber Operations degree program is required to provide curriculum updates at least once per year to verify that the curriculum is staying current in a quickly changing field. The Cyber Operations BAS program at the University of Arizona has included a twice yearly review of curriculum in their documentation to the NSA. A copy of this review process is attached. This review includes a minor review after the end of the Fall semester, and a more stringent review at the end of the Spring semester each year. This provides the opportunity for minor revisions before a course may be taught again, and time for more major adjustments during the summer prior to courses resuming in the Fall semester.

VIII. NEED FOR THE MAJOR—describe how the major fulfills the needs of the city, state, region, and nation. Provide market analysis data or other tangible evidence of the need for and interest in the proposed major. This might include results from surveys of current students, alumni, and/or employers or reference to student enrollments in similar programs in the state or region. Include an assessment of the employment opportunities for graduates of the program during the next three years. According to the Bureau of Labor Statistics, the rate of growth for jobs in cybersecurity is projected at 37% from 2012–2022—much faster than the average for all other occupations. The field of Cybersecurity in the U.S. employed nearly 780,000 people in 2017 yet still maintains a 0% unemployment rate. The Bureau of Lab Statistics noted that over 350,000 cybersecurity position still remain unfilled and estimates that the shortage of cyber professionals in the U.S. will grow to over 3.5 million by 2021. Additionally, according to the National Initiative for Cybersecurity Education (NICE), the demand for cybersecurity talent will increase annually by approximately 1.5 million jobs globally through 2022. UA South’s existing program has already generated more than 240 declared majors after only five (5) semesters since the inception of the BAS in Applied Science with a Cyber Operations emphasis. The reason this degree program has been—and will continue to be—one of the most popular programs at the University of Arizona is that it is preparing students for a career field in which the number of open positions far outweighs the number of qualified applicants.
IX. ANTICIPATED STUDENT ENROLLMENT - complete the table below. What concrete evidence/data was used to arrive at the numbers?

<table>
<thead>
<tr>
<th>5-YEAR PROJECTED ANNUAL ENROLLMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>1</strong>&lt;sup&gt;st&lt;/sup&gt; Year</td>
</tr>
<tr>
<td>Number of Students</td>
</tr>
</tbody>
</table>

Data/evidence used to determine projected enrollment numbers: The UA Cyber Operations program has more than 240 declared majors after only five (5) semesters since the inception of the BAS in Applied Science with a Cyber Operations emphasis. The program was recently designated as one of twenty (20) of the National Security Agency’s National Centers of Academic Excellence in Cyber Operations (https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/), and one of the nine (9) Department of Defense Servicemembers Opportunity College (SOC) (https://www.gosoced.org) Cybersecurity program founding members, making it one of the top Cyber programs in the Nation. The rate of enrollment has increased every semester and shows no signs of slowing down in the immediate future. Due to the increasing demand for highly qualified cyber professionals and the growing awareness of the UA Cyber Operations program, we believe the estimated rate of growth underpinning the anticipated student enrollment numbers are conservative.

X. ANTICIPATED DEGREES AWARDED - complete the table below, beginning with the first year in which degrees will be awarded. How did you arrive at these numbers? Use National Center for Education Statistics College Navigator to find program completion information of peer institutions offering a same or similar major.

<table>
<thead>
<tr>
<th>PROJECTED DEGREES AWARDED ANNUALLY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>1</strong>&lt;sup&gt;st&lt;/sup&gt; Year</td>
</tr>
<tr>
<td>Number of Degrees</td>
</tr>
</tbody>
</table>

The Anticipated Degrees Awarded projections are based on a combination of factors: first, the anticipated graduation rate of our existing full and part-time Junior/Senior student population within the Cyber Operations program; second, program completion statistics from similar BAS programs found at the National Center for Education Statistics (NCES); and finally, a
comparison of program completion statistics from other NSA designated Center of Academic Excellence in Cyber Operations (CAE-CO) programs. Due to the robustness of our program, the innovative delivery of our courses via the Cyber Virtual Learning Environment, and the increasing demand for highly qualified cyber professionals, we believe the estimated rate underpinning the anticipated degrees awarded annually numbers are conservative.

XI. PROGRAM DEVELOPMENT TIMELINE- describe plans and timelines for 1) marketing the major and 2) student recruitment activities.
Because its offices and classrooms are located on, or near, community college campuses, UAS defines its markets first by geographic segmentation. Demographics and other relevant factors narrow its target audience to those groups of people to whom UAS can offer the greatest value, while realizing positive, sustainable return on investment. The target audience consists of prospective transfer students, largely those who are considered to be non-traditional students. This population includes students who are currently working full-time or nearly full-time, those who are parents or are caring for other family members including aging parents, and military personnel (including those who are currently deployed). Our students are primarily location-bound with strong ties to family and community within southern Arizona. Our prospective student population is results oriented and career focused, with an average age range of 21-35 years of age.

1) The Cyber Operations program is already a robust existing program with over 240 declared majors. We have implemented an initial marketing plan that consists of the following:
   a. UA Cyber Operations program website located at: https://cyber-operations.uas.arizona.edu. Our program website provides detailed information on: our National Security Agency (NSA) designation as a National Center of Academic Excellence in Cyber Operations (CAE-CO); detailed information on our two existing subplans (Cyber Engineering and Defense & Forensics) to include sample program schedules and course descriptions/learning outcomes; the UA CyberApolis Cyber Virtual Learning Environment; Cyber Operations Career information; Cyber Operations Faculty; and admissions requirements. Our Cyber Operations program website links to the UA Main website and the UA admissions application website.
   b. The Cyber Operations program is also fully integrated into Arizona Online and its website located at: https://uaonline.arizona.edu/programs/undergraduate/online-bachelor-applied-science-cyber-operations-applied-science-bas. This website provides high level details on the Cyber Operations program, a program video, and links to admissions and the application. This site also provides links back to the UA Cyber Operations program website.
   c. The UA Cyber Operations program is also prominently displayed on the front/landing page of the CyberDegrees.org website located at: https://www.cyberdegrees.org/listings/best-online-cyber-security-
This site lists the “18 Best Online Cyber Security Bachelor’s Degrees in 2018”. This site directly links to the Arizona Online’s Cyber Operations website listed above. The Cyber Degrees website also provides high level details on the Cyber Operations program and our Cyber Virtual Learning Environment.

d. The UA Main website does contain links to the Cyber Operations program under the Degree Search page located at: https://degreesearch.arizona.edu/major/applied-science-cyber-operations-emphasis. This page links to the UA South Applied Science: Cyber Operations Emphasis page. The UA Main website will need to be updated with a direct link to the Cyber Operations program once it becomes its own BAS degree.

e. The UA Admissions “Pathways to the UA” webpage has no direct path to the Cyber Operations page. However, given a detailed, labor-intensive search, the Cyber Operations program can be found under the Degree Search page. The UA Admissions website will need to be updated with a direct link to the Cyber Operations program once it becomes its own BAS degree.

f. The Cyber Operations program has developed a detailed program brochure. The brochure is a multifold 10-page document that provides most of the information from the Cyber Operations program website as well as contact information for Admissions and the Cyber Operations program office. This brochure is given out at various Student Services and Cyber Operations program recruiting events. They are also made available on the UA South campus.

g. UA South has also developed a one-page Cyber Operations pamphlet with high level program details and contact information for both Admissions and the Cyber Operations program office. These pamphlets are given out at various Student Services and Cyber Operations program recruiting events. They are also made available on the UA South campus.

h. UA South Student Services has also included the Cyber Operations program in its IT Industry academic program pamphlet and marketing materials. The pamphlet is given out at various Student Services and Cyber Operations program recruiting events. They are also made available on the UA South campus.

i. UA South Student Services also markets the Cyber Operations program through their monthly newsletter that goes to current and prospective students.

j. Finally, the Cyber Operations program has developed a detailed web-magazine-like monthly newsletter called “The Packet”. The Packet is sent to all current, prospective, and graduated Cyber Operations Students. The Packet is also sent to all of the Cyber Operations industry, government, and transfer pathway academic partner institutions. The Packet is a 20 to 40-page document that provides students details on: Major Cyber related events for the month; upcoming semester course offerings; UA Spotlight on two or more of our Cyber Operations Faculty; important dates and program information; cyber certification opportunities; 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 Student Services Team, our promotion and communication efforts will focus on raising awareness of the value of obtaining a degree in Cyber Operations, along with generating interest in and providing information about career opportunities for cyber 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 Cyber Operations department to complete their BAS degree. In addition, our Student Services 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 Student Services 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 UAS website where visitors can search for information and begin engaging with the college. From the UAS 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 UAS and University of Arizona Online, to learning more about the nationally-recognized caliber of the curriculum of the Cyber Operations BAS.

XII. DIVERSITY AND INCLUSION—describe how you will recruit diverse students and faculty to this program.

The BAS-CO program is committed to achieving excellence through cultural diversity and actively seeks culturally diverse faculty and students. The current BAS subplan In Cyber Operations demonstrates this commitment: 43% of students identify as Non-White; 20% are female, and 54% are first generation college students. The UA South BAS programs are uniquely able to serve nontraditional transfer student populations, and work in a deeply embedded way within local communities due to a variety of factors, including UA South’s status as a designated branch campus; its continuing designated Hispanic Serving Institution, its founding membership in the Servicemembers Opportunity Colleges (SOC) Cybersecurity Program, and its
physical presence within numerous local communities (including in the Army Education Center at Ft. Huachuca).

<table>
<thead>
<tr>
<th>Name of Proposed Degree (degree type and major), College/School, Location, Anticipated Catalog Year</th>
<th>Program Fee Required? (Yes or No)</th>
<th>Brief Description Justification and Identified Market Need</th>
<th>Learning Outcomes and Assessment Plan</th>
<th>Projected 3rd Year Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bachelor of Applied Science in Cyber Operations, with Subplans in Cyber Engineering, Defense/Forensics, and Cyber Law and Policy University of Arizona South, Arizona Online, UA Distance, Anticipated Catalog Year: 2019-20</td>
<td>No</td>
<td>Description: The BAS in Cyber Operations is designed specifically to prepare graduates for entry into a number of cyber-related occupations in defense, law enforcement, and private industry. The curriculum will provide students with a critical baseline of technology skills, as well as critical thinking skills and detective-like thought processes that enable students to analyze problems and render solutions. Students will apply knowledge of human and organizational behavior to predict vulnerabilities created by human error; understand and know how to apply legal and ethical standards to the world of cyber, and be able to communicate effectively.</td>
<td>Learning Outcome # Operating Systems &amp; Low Level Programming: Demonstrate a thorough understanding of various operating systems and be able to develop low level applications with the required complexity and sophistication to implement exploits for discovered vulnerabilities. Malware Reverse Engineering: Safely perform static and dynamic analysis of unknown software, including obfuscated malware, to fully understand the software’s functionality. Offensive Cyber Operations: Explain and demonstrate the phases of offensive cyber operations; what each phase entails; who has the authorities to</td>
<td>600</td>
</tr>
<tr>
<td></td>
<td>Justification: The BAS is overall the largest and fastest-growing area of enrollment at UA South. It is designed as an opportunity for students to complete a bachelor's degree with all of the knowledge and skills necessary to be immediately employable in a professional field. The BAS is structured with a set of core courses designed to meet certain requirements identified by employers as essential knowledge and skills for success in the workplace. These core requirements are technical writing, critical thinking, research and analysis, applied mathematics, professional ethics, and a capstone experience synthesizing and applying knowledge learned in the content area. Although these core requirements have not changed since the BAS was first implemented, the addition of new subplans in diverse content areas has resulted in different courses being proposed to meet these requirements. While the intent behind requiring specific courses to meet the BAS core requirements was to provide a better alignment of the core requirements to the content of the subplans, the end result has been to cause the BAS degree to be out of compliance with ABOR policy requiring a certain percentage of identical courses within conduct each phase; and how operations are assessed after completion.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Defensive Cyber Operations:</strong></td>
<td>Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Forensics:</strong></td>
<td>Demonstrate and explain how to acquire a forensically sound image; understand user activity; determine the manner in which an operating system or application has been subverted; identify forensic artifacts left by attacks; and recover deleted and/or intentionally hidden information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Networking:</strong></td>
<td>Demonstrate a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Critical Thinking &amp; Problem Solving:</strong></td>
<td>Demonstrate understanding of how variability affects outcomes; how to identify anomalous events; how to integrate and differentiate continuous functions of multiple variables; and how</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
a single major. Accordingly, what are currently subplans within the single BAS degree program are being reorganized into BAS degree programs aligned into appropriate content majors. The BAS subplan of Cyber Operations—Engineering track and Cyber Operations, Defense/Forensic track—which currently have approximately 240 majors combined—are being reorganized into a BAS in Cyber Operations with subplans in Cyber Engineering, Defense/Forensics, and an additional subplan in Cyber Law and Policy. The existing subplans are steadily increasing in enrollment at all locations in which they offered. The proposed subplan in Cyber Law and Policy is comprised of the same core courses as the other two subplans, but will allow students to specialize in the growing field of cyber law and policy by combining courses currently offered in the BAS in Cyber Operations with courses from the Government and Public Service program.

Market Need: There are currently 240 declared majors after only four (4) semesters since the inception of the BAS in Applied Science with a Cyber Operations emphasis. The program was recently designated as one of to solve complex problems using computation and scripting languages.

Law, Ethics, & Policy: Describe and explain the relationship between cyber ethics and law; US and International cyber laws; criminal penalties related to unethical hacking; and apply the notion of Gray Areas to articulate where the law has not yet caught up to technology innovation.

Security Principles & Vulnerabilities: Demonstrate and explain the various types of vulnerabilities and their underlying causes; how security principles interrelate and are typically employee to achieve assured solutions; and explain how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.

Cyber Threat Intelligence: Describe and demonstrate how knowledge about an adversary’s motivation, intentions, and methods are collected, analyzed, and disseminated to help security personnel and business staff to align resources and protect critical assets within an enterprise architecture.
twenty (20) of the National Security Agency’s National Centers of Academic Excellence in Cyber Operations, and one of the nine (9) Department of Defense Servicemembers Opportunity College (SOC) Cybersecurity program founding members. The reason this degree program has been—and will continue to be—one of the most popular programs at the University of Arizona is that it is preparing students for a career field in which the number of open positions far outweighs the number of qualified applicants. The cybersecurity unemployment rate within the US has been zero percent (0%) for the past 18 months. In 2017 the U.S. employed nearly 780,000 people in cybersecurity positions, with approximately 350,000 unfilled cybersecurity openings. According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37% from 2012–2022—much faster than the average for all other occupations. According to the National Initiative for Cybersecurity Education (NICE), the demand for cybersecurity talent will increase annually by approximately 1.5 million jobs globally through 2022.

<table>
<thead>
<tr>
<th>Assessment Method and/or Instrument(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CYBV 301—Fundamentals of Cybersecurity is the gateway course for the BAS in Cyber Operations (BAS-CO). Students will take a pre-test (multiple choice and short answer) at the start of this course on the content addressed in Program Student Learning Outcomes (ELOs). Students will also be asked to self-assess their level of knowledge of the study of cybersecurity principles and what they expect to know and be able to do at the end of the Cyber Operations program. This pre-test will measure both direct and indirect evidence of student prior knowledge. A post-test assessing the same content will be administered to students in their culminating/capstone course, assessing student mastery of the ELOs. The pre-test will establish a baseline from which to judge how well the Cyber Operations program meets the objectives articulated in the ELOs.</td>
</tr>
</tbody>
</table>
| 2. There are three subplans in the BAS-CO program and students in the respective subplan must take the CYBV 301 Fundamentals of Cybersecurity gateway course. All courses that meet the subplan requirements in the BAS-CO program include knowledge-based and/or performance-based assessments where the student must demonstrate
they have mastered the knowledge, skills and abilities that are assessed according to the standard program analytic rubric through D2L and the UA Cyber Virtual Learning Environment. Assessment data will be collected through the application of this rubric for the gateway course and all of the core elective courses within a single subfield on a yearly basis and will be analyzed to determine if students achieved the designated ELOs.

3. CYBV 498—Senior Capstone: during this course students propose, develop, and complete comprehensive and cumulative performance-based research projects. These projects will provide data that will be used to assess whether students have acquired the knowledge, skills, and abilities that comprise the ELOs expected of the BAS-CO program. Student mastery of these outcomes will be assessed through an evaluation of the final performance-based research project according to the capstone analytic rubric through D2L and the UA Cyber Virtual Learning Environment. Assessment data collected through the application of this rubric to Senior Capstone Research Projects will be analyzed on an ongoing basis.

4. As noted above, students in CYBV 498 will take a subplan-appropriate program
post-test that reassesses their content knowledge and asks them to rate the knowledge, skills, and abilities contained in the ELOs that they have acquired as a result of completing the BAS-CO Program. Students will also be asked whether learning outcomes for the program were clear; whether course content and materials, activities, assignments, and tests in their classes contributed to meeting the ELOs of the BAS-CO program. Finally, students will be asked what are the three most important things they learned in the BAS-CO program. This information will be compiled and analyzed against the Pre-survey data.
Appendix A. Minor Requirements. Complete if requesting a minor (must have same name). Delete EXAMPLE column before submitting.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total units required to complete minor</td>
<td>N/A</td>
</tr>
<tr>
<td>Upper-division units required</td>
<td>N/A</td>
</tr>
<tr>
<td>Total transfer units that may apply to minor</td>
<td>N/A</td>
</tr>
<tr>
<td>List any special requirements to declare/admission to this minor</td>
<td>N/A</td>
</tr>
<tr>
<td>(completion of specific coursework, minimum GPA, interview, application, etc.)</td>
<td></td>
</tr>
<tr>
<td>Minor requirements (list all required coursework including core and electives)</td>
<td>N/A</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Internship, practicum, applied course requirements (yes/no). If yes, provide description.</td>
<td>N/A</td>
</tr>
<tr>
<td>Additional requirements (provide description)</td>
<td>N/A</td>
</tr>
<tr>
<td>Any double-dipping restrictions? (Yes/No. If yes, provide description)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Appendix B. Faculty CV. Complete the table below by providing UA Vitae profile link or short CV for each faculty member participating in the proposed program. Add rows as needed. UA Vitae profiles can be found in the [UA directory/phonebook](#).

<table>
<thead>
<tr>
<th>Full Time Faculty Member</th>
<th>UA Vitae link or “CV attached”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jason Denno, M.S., M.B.A.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Paul Wagner, M.S., M.B.A.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Thomas Jewkes, M.S.</td>
<td>CV attached</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adjunct Faculty Members</th>
<th>CV attached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elke Drennan, Ph.D.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Harry Cooper, Ph.D.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Mohamed Meky, Ph.D.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Heidi Calhoun-Lopez, JD</td>
<td>CV attached</td>
</tr>
<tr>
<td>Robert Batey, JD</td>
<td>CV attached</td>
</tr>
<tr>
<td>Rock Stevens, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Luis Mendieta, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Troy Ward, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Ture Peken, M.S./ABD</td>
<td>CV attached</td>
</tr>
<tr>
<td>David Drennan, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Jordan VanHoy, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Kate Mabbett, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Henry Werchen, M.S.</td>
<td>CV attached</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Faculty Members from Other BAS Programs</th>
<th>CV attached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linda Denno, Ph.D.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Li Xu, Ph.D.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Odile Wolf, M.S.</td>
<td>CV attached</td>
</tr>
<tr>
<td>Sandra Moore, M.S.</td>
<td>CV attached</td>
</tr>
</tbody>
</table>
Appendix C. Sample Curriculum Map for BA in Statistics and Data Science. Created using taskstream. Contact OIA for assistance in creating your curriculum map.
Appendix D. Assessment Plan for Student Learning

To assess student learning outcomes from the beginning of their time in the BAS Cyber Operations to the end of their BAS degree, the Cyber Operations Program Office will provide an evaluation to each student to determine their knowledge of Cyber Operations, Cyber Security, Computer Programming and Digital Forensics subject matter. When they are a new student, the Cyber Operations Program Office will ask each student to complete an evaluation of their knowledge of Cyber topics by completing a questionnaire in their first CYBV course (typically CYBV 301 or CYBV 385). To ensure that these assessments are completed, we would request that all new students be placed in a Student Group that will place an Advising Hold on the student accounts that may not be lifted until students complete the assessment. This will serve as their base score for their subject matter knowledge when beginning the degree program. At the end of the student’s degree program, when they register for the program capstone course (CYBV 498) we will request that they be placed in another Student Group that will then place a Hold on their account that will not allow their final degree audit to be completed for graduation if they have not yet completed a questionnaire on their subject matter knowledge at the end of their degree program. The content for this assessment will be pulled from a question bank generated by compiling quiz, midterm, and final exam questions from all CYBV courses required for completion of the Cyber Operations BAS degree program.

In addition, to provide information to the Program Director, faculty members, and Advisory Board, the Cyber Operations Program Office will administer surveys to the current students in the Cyber Operations degree program at the end of each Fall and Spring semester. A draft of this survey instrument is included, and is designed to provide more general information about student opinions on the degree program’s course offerings and scheduling options. This survey information will be emailed out by the Program Manager for Cyber Operations at the end of each Fall and Spring, after finals are completed and submitted and will augment the data collected in the specific course TCEs.

Appendix E. Student Learning Assessment Survey Example (Attached)

Appendix F. Program Assessment Graduate/Alumni Survey Example (Attached)

Appendix G. Cyber Operations Curriculum Review & Modification Policy (Attached)

Appendix H. Faculty CVs (Attached)

Appendix I. The Packet (Attached)
## METRICS

<table>
<thead>
<tr>
<th>Metric</th>
<th>1st Year 2019-2020</th>
<th>2nd Year 2020-2021</th>
<th>3rd Year 2021-2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net increase in annual college enrollment UG</td>
<td>31</td>
<td>47</td>
<td>70</td>
</tr>
<tr>
<td>Net increase in college SCH UG</td>
<td>372</td>
<td>567</td>
<td>840</td>
</tr>
<tr>
<td>Net increase in annual college enrollment Grad</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net increase in college SCH Grad</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of enrollments being charged a Program Fee</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Sponsored Activity (MTDC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Faculty FTE</td>
<td>5.75</td>
<td>6.00</td>
<td>6</td>
</tr>
</tbody>
</table>

## FUNDING SOURCES

### Continuing Sources

<table>
<thead>
<tr>
<th>Source</th>
<th>1st Year 2019-2020</th>
<th>2nd Year 2020-2021</th>
<th>3rd Year 2021-2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>UG RCM Revenue (net of cost allocation)</td>
<td>300,407</td>
<td>450,610</td>
<td>675,915</td>
</tr>
<tr>
<td>Grad RCM Revenue (net of cost allocation)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program Fee RCM Revenue (net of cost allocation)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F and A Revenues (net of cost allocations)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arizona Online Revenues</td>
<td>467,719</td>
<td>701,578</td>
<td>1,052,367</td>
</tr>
<tr>
<td>Distance Learning Revenues</td>
<td>97,020</td>
<td>145,530</td>
<td>218,295</td>
</tr>
<tr>
<td>Reallocation from existing College funds (attach description)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Items (attach description)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Continuing</strong></td>
<td>$865,146</td>
<td>$1,297,718</td>
<td>$1,946,577</td>
</tr>
</tbody>
</table>

### One-time Sources

<table>
<thead>
<tr>
<th>Source</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>College fund balances</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Institutional Strategic Investment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gift Funding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Items (attach description)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total One-time</strong></td>
<td>$</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>TOTAL SOURCES</strong></td>
<td>$865,146</td>
<td>$1,297,718</td>
<td>$1,946,577</td>
</tr>
</tbody>
</table>

## EXPENDITURE ITEMS

### Continuing Expenditures

<table>
<thead>
<tr>
<th>Item</th>
<th>1st Year 2019-2020</th>
<th>2nd Year 2020-2021</th>
<th>3rd Year 2021-2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>400,000</td>
<td>415,000</td>
<td>435,000</td>
</tr>
<tr>
<td>Other Personnel</td>
<td>65,000</td>
<td>65,000</td>
<td>65,000</td>
</tr>
<tr>
<td>Employee Related Expense</td>
<td>134,150</td>
<td>137,300</td>
<td>141,500</td>
</tr>
<tr>
<td>Graduate Assistantships</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Graduate Aid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations (materials, supplies, phones, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Space Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Items (attach description)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Continuing</strong></td>
<td>$599,150</td>
<td>$617,300</td>
<td>$641,500</td>
</tr>
</tbody>
</table>

### One-time Expenditures

<table>
<thead>
<tr>
<th>Item</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Construction or Renovation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start-up Equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replace Equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Library Resources</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Items (attach description)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total One-time</strong></td>
<td>$</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>TOTAL EXPENDITURES</strong></td>
<td>$599,150</td>
<td>$617,300</td>
<td>$641,500</td>
</tr>
</tbody>
</table>

**Net Projected Fiscal Effect**

<table>
<thead>
<tr>
<th></th>
<th>1st Year 2019-2020</th>
<th>2nd Year 2020-2021</th>
<th>3rd Year 2021-2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Projected Fiscal Effect</td>
<td>$265,996</td>
<td>$680,418</td>
<td>$1,305,077</td>
</tr>
</tbody>
</table>
### Undergraduate Major Peer Comparison Chart

Delete **EXAMPLE columns** once ready to submit/upload. Find UA peers here: [https://www.azregents.edu/arizonas-public-universities/peer-institutions](https://www.azregents.edu/arizonas-public-universities/peer-institutions)

<table>
<thead>
<tr>
<th>Program name, sub-plan name (if applicable), degree, and institution</th>
<th>Proposed UA Program:</th>
<th>Peer 1:</th>
<th>Peer 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major: Cyber Operations</td>
<td><strong>Dakota State</strong></td>
<td><strong>Texas A&amp;M</strong></td>
<td></td>
</tr>
<tr>
<td>Subplans: Cyber Engineering Defense/Forensics Cyber Law and Policy</td>
<td>Current NSA CAE-CO Program</td>
<td>Current NSA CAE-CO Program</td>
<td></td>
</tr>
<tr>
<td>Bachelor of Applied Science degree, UA South</td>
<td>Major: B.S. Cyber Operations</td>
<td>Major: B.S. in Computer Science, Minor in Cybersecurity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The requirements to fulfill the NSA CAE-CO designation are met by the Engineering Track minor in Cybersecurity. Texas A&amp;M does not have a major degree program in Cybersecurity or Cyber Operations, but is a University of Arizona peer public university with an NSA designation as a CAE-CO.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current # of enrolled students</th>
<th>120 units</th>
<th>126 units + 16 units for the Cybersecurity Minor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Description - provide a description for the proposed program. Include the purpose, nature, and program</td>
<td>The BAS in Cyber Operations prepares graduates for cyber-related occupations in defense, law enforcement, and private industry. The curriculum</td>
<td>From: <a href="https://dsu.edu/academics/degrees-and-programs/cyber-operations-bs">https://dsu.edu/academics/degrees-and-programs/cyber-operations-bs</a></td>
</tr>
<tr>
<td>Description of major</td>
<td>Because data breaches, malware infections, and software vulnerabilities are so common in today’s</td>
<td></td>
</tr>
</tbody>
</table>
| highlights. Description must be consistent throughout the proposal documents and match departmental and college websites, handouts, and promotional materials. | includes both offensive and defensive cyber security content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure our students have extensive hands-on experiences to develop the knowledge, skills, and abilities necessary to succeed after they graduate. The BAS degree in Cyber Operations offers three subplans, both in-person and fully online: Cyber Engineering, Defense and Forensics, and Cyber Law and Policy. | technology world, it is critical to fully understand how these attacks take place. As a cyber operations major (offered on campus and online), you will dig deep to understand the mentality, motivations, and techniques of the hackers that execute these types of attacks.

You will start with a strong base of programming, math, and networking and then apply that knowledge to the most technical areas of cyber security. At the core of the degree, you learn how reverse engineering works, analyze malware and exploit software. You will better understand the hacker mindset and be able to discover vulnerabilities in widespread computer systems. | Machinery recommendations for curricula and courses. The four-year undergraduate curriculum in computer science includes a sound preparation in science, mathematics, English, statistics and computing. Students majoring in computer science at Texas A&M will take a 12-hour area of concentration in another department. Electives are available in the areas of: algorithms, languages and computability, software systems, networking, computer systems and architecture, artificial intelligence and cognitive modeling, vision, graphics and robotics and computational science and engineering. Advanced undergraduates may take graduate courses in these areas.

Our mission is to prepare intellectual, professional, and ethical graduates capable of meeting challenges in the field of computer science; and to coordinate with other parts of the university to facilitate the effective use of educational resources, including courses.

The Cybersecurity Minor is designed to appeal to both less technically-oriented and more technically-oriented undergraduate students, across multiple departments, in multiple colleges. All students who enroll in the minor will acquire a basic understanding of programming, and a firmly grounded understanding of cybersecurity, to include cyber ethics. The inclusion of these courses in the minor will allow students to specialize in the area of cybersecurity that is most closely aligned with their respective interests and their degree plans. |
| Target careers | • Cyber Engineering  
• Lead Security Engineer  
• Cybersecurity Engineer  
• Vulnerability Analyst  
• Security Architect  
• Application Security Manager | • Lead Security Engineer  
• Cybersecurity Engineer  
• Vulnerability Analyst  
• Security Architect  
• Application Security Manager | • Computer Scientist  
• Software Engineer  
• Lead Security Engineer  
• Cybersecurity Engineer  
• Vulnerability Analyst  
• Security Architect  
• Application Security Manager |
<table>
<thead>
<tr>
<th>Foundation courses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>English composition</strong></td>
</tr>
<tr>
<td>ENGL 101 (3) First-Year Composition or equivalent</td>
</tr>
<tr>
<td>ENGL101 Written Communication (3 units)</td>
</tr>
<tr>
<td>ENGL201 Written Communication (3 units)</td>
</tr>
<tr>
<td>ENGL 103 Introduction to Rhetoric and Composition (3 units) or ENGL 104 Composition and Rhetoric (3 units)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total units required to complete degree</th>
<th>120 units</th>
<th>120 units</th>
<th>142 units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper-division units required to complete degree</td>
<td>45 units</td>
<td>48 units</td>
<td>58 units</td>
</tr>
</tbody>
</table>

- Total units required to complete degree: 120 units, 120 units, 142 units.
- Upper-division units required to complete degree: 45 units, 48 units, 58 units.
- English composition:
  - ENGL 101 (3) First-Year Composition or equivalent
  - ENGL101 Written Communication (3 units)
  - ENGL201 Written Communication (3 units)
  - ENGL 103 Introduction to Rhetoric and Composition (3 units) or ENGL 104 Composition and Rhetoric (3 units)
- Second language:
  - CYBV 473—Violent Python or CSCV 352—System Programming in Unix or CYBV 470—C Programming for Security Professionals (2nd Semester Programming Language) or 2nd Semester Foreign Language Proficiency
  - None
  - One year of a foreign language—which can be completed at the high school level. No additional foreign language required for this major.
<table>
<thead>
<tr>
<th>Math</th>
<th>BASV 314—Mathematics for Applied Sciences or BASV 376—Discrete Math</th>
<th>MATH 201 - Introduction to Discrete Mathematics (3 units)</th>
<th>Math 302 Discrete Mathematics (3 units)</th>
</tr>
</thead>
<tbody>
<tr>
<td>General education requirements</td>
<td>TIER II GENERAL EDUCATION (21 Units) Natural Sciences (3 Units) Arts and Humanities (6 Units) Individuals and Societies (12 Units) Diversity Requirement</td>
<td>System-wide General Education Requirements (SGE) (30 Units) Written Communication (6 units): -ENGL 101 - Composition I (3 units) -ENGL 201 - Composition II (3 units) Oral Communication (3 units) Social Sciences (6 units) Arts and Humanities (6 Units) Mathematics (3 Units) Natural Sciences (6 units)</td>
<td>Communication (6 units) Mathematics (6 units) Life and Physical Sciences (9 units) Language Philosophy and Culture (3 units) Creative Arts (3 units) American History (6 units) Government/Political Science (6 units) Social and Behavioral Sciences (3 units)</td>
</tr>
<tr>
<td>Pre-major? (Yes/No. If yes, provide requirements.) Provide email(s)/letter(s) of support from home department head(s) for courses not</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
| List any special requirements to declare or gain admission to this major (completion of specific coursework, minimum GPA, interview, application, etc.) | The Cyber Operations program requires a supplemental program application in addition to admission to The University of Arizona. The entrance requirements include:  
- Minimum 2.5 GPA in your college coursework  
- Resume  
- Goal statement  
Cyber Engineering Subplan:  
- AAS in Cybersecurity (recommended) | Minimum required GPA to declare major is 2.0.  
Minimum required GPA to declare minor is a 2.5.  
Must make a grade of 'C' or better in each course used towards minor.  
Must achieve an overall GPA of 2.5 in approved minor coursework.  
Minimum of 6 hours at 300-400 level.
- ECE 175: Computer Programming for Engineering Applications (3 units)
- BASV 300, MATH 243 or CSC 245: Intro to Discrete Math (3 units)

Defense/Forensics and Cyber law and Policies Subplans:
- AAS degree in cybersecurity related field (recommended)

Cyber Engineering Subplan: AAS degree in computer science
<table>
<thead>
<tr>
<th>Major requirements</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum # of units required in major (units counting towards major units and major GPA)</td>
<td>42</td>
<td>78</td>
</tr>
<tr>
<td>Minimum # of upper-division units required in the major (upper division units counting towards major GPA)</td>
<td>39</td>
<td>45</td>
</tr>
<tr>
<td>Minimum # of residency units to be completed in the major</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Required supporting coursework (courses that do not count towards)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Major requirements (list all required major coursework including major core, major electives, sub-plan core, and sub-plan electives)</td>
<td>BAS in Cyber Operations Core (27 units)</td>
<td>B.S. Cyber Operations</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>CYBV 301: Fundamentals Cyber Security (3 units)</td>
<td>The B.S. in Cyber Operations degree requires a total of 72 credit hours in the following courses:</td>
</tr>
<tr>
<td></td>
<td>ENGV 306: Advanced Composition (3 units)</td>
<td>CSC 105 Intro to Computers (3 units)</td>
</tr>
<tr>
<td></td>
<td>INFV 320: Computational</td>
<td>CSC 150 Computer Science I (3 units)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSC 134 Intro to Cyber Operations (3 units)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSC 250 Computer Science II (3 units)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Courses Count Towards Major Units and Major GPA</td>
<td>Courses Offered</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Provide email(s)/letter(s) of support from home department head(s) for courses not owned by your department.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Thinking and Doing (3 units)</strong></td>
<td><strong>CSC 363 Hardware, Virtualization &amp; Data Comm. (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>BASV 314: Mathematics for Applied Science (3 units)</strong></td>
<td><strong>CIS 275 Web Application Programming I (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td>-or- <strong>BASV 376: Mathematics for Applied Technology (3 units)</strong></td>
<td><strong>CSC 234 Web Software Security (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>BASV 326: Intro Methods of Network Analysis (3 units)</strong></td>
<td><strong>CSC 383 Networking I (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>BASV 329: Cyber Ethics (3 units)</strong></td>
<td><strong>CSC 300 Data Structures (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CYBV 385: Intro to Cyber Operations (3 units)</strong></td>
<td><strong>CIS 375 Web App Programming II (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CYBV 400: Active Cyber Defense (3 units)</strong></td>
<td><strong>CSC 385 Networking II (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CYBV 498: Senior Capstone (3 units)</strong></td>
<td><strong>CSC 328 Operating Environments (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Computer Engineering Subplan Core (15 units)</strong></td>
<td><strong>CSC 314 Assembly Language (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CYBV 470: C Programming for Security</strong></td>
<td><strong>CSC 321 Information Security Mgmt (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>COMM 203: Public Speaking (3 units)</strong></td>
<td><strong>CSC 436 Off Network Security (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>COMM 205: Communication for Technical Professions (3 units)</strong></td>
<td><strong>CSC 438 Defensive Network Security (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ENGL 210: Technical and Business Writing (3 units)</strong></td>
<td><strong>CSC 456 Operating Systems (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CSCE 313: Introduction to Computer Systems (4 units)</strong></td>
<td><strong>CSC/CSC elective (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CSCE 315: Programming Studio (3 units)</strong></td>
<td><strong>CSC 404 Foundation of Computation (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CSCE 481: Seminar (1 unit)</strong></td>
<td><strong>CSC 420 Cellular &amp; Mobile Communications (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>STAT 211: Principles of Statistics (3 units)</strong></td>
<td><strong>ENGR 482/PHIL 482: Ethics and Engineering (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CSCE 411: Design and Analysis of Algorithms (3 units)</strong></td>
<td><strong>Computer science electives (18 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Select one from: (3 units)</strong></td>
<td><strong>Science elective (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MATH 251: Engineering Mathematics III (3 units)</strong></td>
<td><strong>Concentration area elective (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MATH 302: Discrete Mathematics (3 units)</strong></td>
<td><strong>The minor in Cybersecurity requires an additional 16 semester credit hours in the following courses:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MATH 308: Differential Equations (3 units)</strong></td>
<td><strong>CSCE 313 Introduction to Computer Systems (4 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CSCE 482: Senior Capstone Design (3 units)</strong></td>
<td><strong>CSCE 315 Programming Studio (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ENGR 482/PHIL 482: Ethics and Engineering (3 units)</strong></td>
<td><strong>CSCE 410 Operating Systems (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Computer science electives (18 units)</strong></td>
<td><strong>CSCE 465 Computer and Network Security</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Science elective (3 units)</strong></td>
<td><strong>And one of the following courses:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Concentration area elective (3 units)</strong></td>
<td><strong>CSCE451 Software Reverse Engineering (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>The minor in Cybersecurity requires an additional 16 semester credit hours in the following courses:</strong></td>
<td><strong>-or-</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CSCE463 Networks and Distributed Processing</strong></td>
<td><strong>CSCE465 Computer and Network Security</strong></td>
<td></td>
</tr>
<tr>
<td><strong>-or-</strong></td>
<td><strong>And one of the following courses:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ECEN424 Fundamentals of Networking (3 units)</strong></td>
<td><strong>CSCE451 Software Reverse Engineering (3 units)</strong></td>
<td></td>
</tr>
<tr>
<td>Professionals (3 units) or CSCV 352: System Programming &amp; Unix (3 units)</td>
<td>CYBV 389: Operating System Theory for Security Professionals or CSCV 452: Principles of Operating Systems (4 units)</td>
<td>CSC 428 Reverse Engineering (3 units)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>CYBV 388: Cyber Investigations &amp; Forensics (3 units)</td>
<td>CYBV 454: Malware Threats &amp; Analysis (3 units)</td>
<td>CSC 432 Malware Analysis (3 units)</td>
</tr>
<tr>
<td>CYBV 471: Assembly Language (3 units)</td>
<td>CYBV 479: Wireless Network &amp; Security (3 units)</td>
<td>CSC 437 Survey of Enterprise Syst (3 units)</td>
</tr>
<tr>
<td>Defense/Forensics Subplan Core (15 units)</td>
<td></td>
<td>CIS/CSC elective (3 units)</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Units</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>CYBV 435</td>
<td>Cyber Threat Intelligence (3 units)</td>
<td></td>
</tr>
<tr>
<td>CYBV 454</td>
<td>Malware Threats &amp; Analysis (3 units)</td>
<td></td>
</tr>
<tr>
<td>CYBV 480</td>
<td>Cyber Warfare (3 units)</td>
<td></td>
</tr>
<tr>
<td>CYBV 436</td>
<td>Choose 1: Counter Cyber Threat Intelligence (3 units)</td>
<td></td>
</tr>
<tr>
<td>CYBV 473</td>
<td>Violent Python (3 units)</td>
<td></td>
</tr>
<tr>
<td>CYBV 477</td>
<td>Advanced Computer Forensics (3 units)</td>
<td></td>
</tr>
<tr>
<td>CYBV 481</td>
<td>Social Engineering Attacks &amp; Defenses (3 units)</td>
<td></td>
</tr>
<tr>
<td>GPSV 314</td>
<td>National Security Policy (3 units)</td>
<td></td>
</tr>
</tbody>
</table>

**Cyber Law and Policy Subplan Core (15 units)**

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPSV 461</td>
<td>Civil Rights and Liberties</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 435</td>
<td>Cyber Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>Choose 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBV 436</td>
<td>Counter Cyber Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>GPSV 441</td>
<td>American Foreign Policy</td>
<td>3</td>
</tr>
<tr>
<td>GPSV 442</td>
<td>International Law</td>
<td>3</td>
</tr>
<tr>
<td>GPSV 471</td>
<td>National Security &amp; Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>GPSV 473</td>
<td>National Security Operations &amp; Issues</td>
<td>3</td>
</tr>
<tr>
<td>GPSV 474</td>
<td>Politics of Terrorism</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 473</td>
<td>Violent Python</td>
<td>3</td>
</tr>
<tr>
<td>Course</td>
<td>Yes/No</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GPSV 496: Special Topics in Regional Politics and Security (3 units)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internship, practicum, applied course requirements (Yes/No. If yes, provide description)</td>
<td>Yes</td>
<td>Students must complete CYBV498, Senior Capstone, with a minimum 45 hour student engagement experience.</td>
</tr>
<tr>
<td>Senior thesis or senior project required (Yes/No. If yes, provide description)</td>
<td>Yes</td>
<td>Students must engage in a senior project and write a senior project thesis paper as part of the CYBV498—Senior Capstone.</td>
</tr>
<tr>
<td>Additional requirements (provide description)</td>
<td></td>
<td>Students must earn a minimum 2.0 major GPA. <strong>Students in the Cyber Engineering subplan must complete the Cyber Operations Undergraduate</strong></td>
</tr>
</tbody>
</table>
Certificate. In addition to the subplan requirements, the following courses are required for the Cyber Operations Undergraduate Certificate:

- CYBV472 Secure Software Development & Assessment (3 units)
- CYBV389 Operating System Theory for Security Professionals (3 units) or CSCV452 Principles of Operating Systems (4 units)
- NETV379 Cloud Computing (3 units)

| Minor (specify if optional or required) | Optional | Optional | Minor in Cybersecurity is required to fulfill NSA requirements for designation as a Center of Academic Excellence in Cyber Operations. |

*Note: comparison of additional relevant programs may be requested.*
Student Learning Assessment Survey

The Cyber Operations Program Office wants to collect data from our current students about their experience in the degree program, as well as the longer-term benefits of completing the degree. We ask that you answer these brief questions so that we may be able to learn how we can continuously improve the degree program for future students. Thank you for helping us!

We will begin with some demographic questions just to get an idea of who our students are and a bit about their backgrounds.

- This semester, did you complete your coursework entirely online, with no courses in person?
  - If yes, were you:
    - UA Online Student
    - UA South or UA Distance Student
- Can you describe your student schedule this semester?
  - Full time (12 credit hours or more per fall or spring semester)
  - Part time (12 credit hours or fewer per fall or spring semester)
- Are you a first generation student (your parents and grandparents did not graduate from college)?
  - Yes
  - No
- Gender
  - Female
  - Male
  - Prefer not to report
- Ethnicity
  - Asian or Asian Indian
  - Black or African American
  - Latino/a, Hispanic, or Chicano/a
  - Native American
  - Native Hawaiian or Pacific Islander
  - White or Caucasian, non-Hispanic
  - Two or more races
  - Prefer not to report
• Military/Veteran status
  o Current military member (active duty or reserves)
  o Veteran
  o Veteran/Military dependent
• What is your current location?
  o Arizona
  o US, not Arizona (please list state)
  o Outside the US
• We would like to help connect our current students with our graduates to assist them with networking and learning more about the industry. Would you be interested in being connected with an alum for networking and mentorship?
  o Yes
  o No

In this section, we would like to ask a little bit about your current employment situation. This data will only be used by the department to provide additional context to understand who our students are and some of their time commitments outside of their classes.

• Are you currently employed in your degree field?
  o If yes, how would you describe your employment sector? Please choose the best answer below:
    ▪ Nonprofit sector
    ▪ Private sector, not defense contracting
    ▪ Private sector defense contracting
    ▪ Government, non-military
    ▪ Military
  o If no, have you sought employment in your degree field? Please choose the best answer below:
    ▪ Yes, I am currently looking for employment in my degree field
    ▪ No, I am currently focusing only on completing my degree
    ▪ Other, please explain

• Are you currently employed outside your degree field?
  o If yes, please describe your workload, on average:
    ▪ I work full time (more than 30 hours per week)
    ▪ I work part time over (15 – 30 hours per week)
    ▪ I work part time (fewer than 15 hours per week)
For this section, we would like to learn more about your experience as a student DURING THE CURRENT SEMESTER. Please respond according to the course(s) in which you were registered this semester.

- I took courses in the Seven Week Session format:
  - Yes
    - If yes, did you feel the Seven Week Session format provided adequate time to learn the course content?
      - Yes
      - No
    - If yes, why did you choose to take courses in the Seven Week Session format?
      - The course was only offered in this format
      - I prefer to take courses in the Seven Week Session format
      - It depends upon the course/content/instructor
  - No
    - If no, why did you choose not to take courses in the Seven Week Session format?
      - The course was not offered in this format
      - I prefer to take courses in the full semester (16 week) format
      - It depends upon the course/content/instructor

- In your classes that were taught online, did you find the synchronous lectures to be beneficial?
  - Yes, I like being in lecture with my classmates and having the chance to interact with them and the instructor
  - No, I did not find them very helpful
  - Not applicable (I did not participate in synchronous lectures)

- Did you find your courses to be appropriately challenging?
  - Yes, they were about as difficult as I expected.
  - No, they were much more difficult than I expected.
  - No they were much less difficult than I expected.

- Did you find your faculty and/or advisors to be helpful in choosing your courses and providing assistance as needed during the semester?
  - Yes
  - No

- Do you feel your previous coursework prepared you for the amount and type of math you would need to do this semester?
  - Yes
  - No
- Do you feel your previous coursework prepared you for the amount and type of computer programming you would need to do this semester?
  - Yes
  - No

In these final questions, we would like to give you the opportunity to provide us with any other information you would like.

- Is there anything you would like to tell the department about your student experience? This can include any suggestions of workshops or programming you would recommend for the department to incorporate.

- Should the department consider any changes to the curriculum or additional course offerings to meet industry needs?

- Is there anything else you would like to tell us?

Thank you for taking the time to complete this brief questionnaire. We appreciate the feedback and your interest in helping us to make continuous improvements to the Cyber Operations degree programs!
Program Assessment Graduate/Alumni Survey

The Cyber Operations Program Office wants to collect data from our graduates about their experience in the degree program, as well as the longer-term benefits of completing the degree. We ask that you answer these brief questions so that we may be able to learn how we can continuously improve the degree program for future students. Thank you for helping us!

We will begin with some demographic questions just to get an idea of who our graduates are and a bit about their backgrounds.

- Did you complete your coursework entirely online, with no courses in person?
  - If yes, were you:
    - UA Online Student
    - UA South or UA Distance Student

- Can you describe your student schedule?
  - Full time (12 credit hours or more per fall or spring semester)
  - Part time (12 credit hours or fewer per fall or spring semester)
  - Combination (some semesters I was full time, some I was part time)

- Are you a first generation student (your parents and grandparents did not graduate from college)?
  - Yes
  - No

- Gender
  - Female
  - Male
  - Prefer not to report

- Ethnicity
  - Asian or Asian Indian
  - Black or African American
  - Latino/a, Hispanic, or Chicano/a
  - Native American
  - Native Hawaiian or Pacific Islander
  - White or Caucasian, non-Hispanic
  - Two or more races
  - Prefer not to report
• Military/Veteran status
  o Current military member (active duty or reserves)
  o Veteran
  o Veteran/Military dependent
• Have you ever held a security clearance?
  o If yes, is it current or expired?
    ▪ Current
    ▪ Expired
• Have you ever held any professional certifications in the Information Technology or Cyber field?
  o If yes, which did you hold?
    ▪ Security +
    ▪ Certified Ethical Hacker (CEH)
    ▪ Certified Information Systems Security Professional (CISSP)
    ▪ CompTIA Advanced Security Practitioner (CASP)
    ▪ SANS Certifications (please list)
  o If yes, which of your certifications are current?
    ▪ Security +
    ▪ Certified Ethical Hacker (CEH)
    ▪ Certified Information Systems Security Professional (CISSP)
    ▪ CompTIA Advanced Security Practitioner (CASP)
    ▪ SANS Certifications (please list)
• What is your current location?
  o Arizona
  o US, not Arizona (please list state)
  o Outside the US
• We would like to help connect our current students with our graduates to assist them with networking and learning more about the industry. Would you be interested in acting as a mentor to current students or networking with current students and other graduates?
  o Yes
  o No
• Do you want to receive information from the Cyber Operations department about networking events, alumni news, and departmental information, including the monthly newsletter?
  o Yes
  o No
• The best email address for me is: __________________________________________________________
In this section, we would like to gather some information about the role your degree may have played in your employment options. We want to provide our current students with the support they need to succeed in their careers, so any information our graduates can provide will assist us with describing the paths our previous graduates have taken.

- When did you graduate?
  - Less than 1 year ago
  - 1 year to 5 years ago
  - More than 5 years ago
- At the time of your graduation, were you employed?
  - If yes, was your job in your degree field?
  - If no, did you have any job offers at the time of your graduation?
    - If yes, were any or all of these offers in your degree field?
    - If no, were you seeking employment at the time of your graduation?
- Are you currently employed in your degree field?
  - If yes, how would you describe your employment sector? Please choose the best answer below:
    - Nonprofit sector
    - Private sector, not defense contracting
    - Private sector defense contracting
    - Government, non-military
    - Military
  - If no, have you sought employment in your degree field? Please choose the best answer below:
    - Yes, I am currently looking for employment in my degree field
    - Yes, but I am no longer looking for employment in my degree field
    - No, I have chosen to pursue additional education
    - No, I have chosen to work in a different field
    - Other, please explain

In these final questions, we would like to give you the opportunity to provide us with any other information you would like.

- Is there anything you would like to tell the department about your job search? This can include any advice you have for new graduates, or suggestions of workshops or programming you would recommend for the department to incorporate.
Should the department consider any changes to the curriculum or additional course offerings to meet industry needs?

Is there anything else you would like to tell us?

Thank you for taking the time to complete this brief questionnaire. We appreciate the feedback and your interest in helping us to make continuous improvements to the Cyber Operations degree programs!
Cyber Operations Curriculum Review & Modification Policy

Background:
In order to keep the UA Cyber Operations curriculum current and relevant, a standardized course and instructor review process is performed at the end of each course. This process examines the quality and relevance of course content; evaluates the effectiveness of instruction; and incorporates the results of student feedback on formal Teacher/Course evaluation surveys. Due to the rapidly evolving nature of the field of cyber operations, our faculty are committed to staying abreast of current events in cyberspace, new and innovative offensive/defensive cyber operations tactics, techniques, and tools. Each year an interdisciplinary board is assembled to examine our research results, assess current events in offensive/defensive cyber operations tactics, techniques and tools, and analyze input from other Cyber Operations community members. These data are reviewed to identify any programmatic or individual course deficiencies and utilized to support continuous updating of course content and relevance.

Members of the Interdisciplinary Board:
- Cyber Operations Program Director – Interdisciplinary Board Chair
- Network Operations Program Director
- Informatics/Computer Science Program Director
- Bachelor of Applied Science Program Director
- Assistant Dean of Student Services
- Full Time Cyber Operations Faculty
- Adjunct Cyber Operations Faculty
- Interdisciplinary Faculty Who Teach in the Cyber Operations Program
- Cyber Virtual Learning Environment (VLE) Software Engineer
- Ad hoc Cyber Operations Industry Professionals

Course Review Inputs
- NSA CAE-CO Fundamental Program Academic Content Requirements
- Predominant Cyber Trends and Threat Actors in the Last 12 Months
- UA Cyber Operations Research Results
- Cyber Operations Course Materials
- Cyber Operations Course Assessment Results
- Teacher/Course Evaluations for all Cyber Operations and Interdisciplinary Courses
- Cyber VLE Resource Status
Course Review & Updating Process

- The Interdisciplinary Board Chair will convene a Cyber Operations Curriculum Review Board each year at the conclusion of the Spring semester.
- The Cyber Operations Program Office is responsible to set the Review Board agenda and arrange the meeting logistics (location, invitations, etc.).
- The Cyber Operations Program Director will provide an update on the NSA CAE-CO Academic Requirements. Any NSA requirement change that will substantially impact UA’s ability to meet its CAE-CO designation requirements will be identified as a mandatory program update.
- The primary Cyber Threat Intelligence Instructor will provide a Current Trends and Threat Actors brief and will provide any recommendations for course updates based on changes in the threat landscape.
- Each UA Cyber Researcher will present an overview of their current research efforts and identify any recommendations for course modifications based on their findings.
- Each Cyber Operations course will be reviewed to determine if the content is still relevant, if the assessment strategies continue to be appropriate, and if the student engagement plan is effective. The following areas will be reviewed at a minimum:
  - Course Content and Required Resources
  - Course Assessment Statistics
  - Labs, Activities, and Writing Assignments
  - Quizzes, Midterms, and Final Examination
  - Instructor TCE Review
  - VLE Support Requirements
- A list of recommended updates will be developed for each course then voted on by the Review Board. The Cyber Operations Program Director will have the final decision on each recommended course modification.
- The Cyber Operations Program Director will work with the UA leadership to obtain any required resources and will assign course updates to the Cyber Operations faculty for completion.
- The Cyber Operations Program Office will maintain a list of all course update requirements and will track the completion of course modifications.
- The Cyber Operations Program Director will review and approve course updates prior to the next academic year course offering.
- The Cyber Operations Program Office will maintain a repository of each course’s materials to provide historical accounting as well as the ability to revert back to a previous course iteration if required.
SUMMARY OF QUALIFICATIONS

Diversified and experienced leader in problem identification, solution development, program management, marketing, public relations, and funding initiatives. Proven leadership of organizations focused on specific solutions that produce immediate results. Expertise in all aspects of technology development and management for the Departments of Defense and Homeland Security. In depth expertise in ground and air based sensors, sensor fusion, data management and visualization, ISR synchronization as well as Tagging, Tracking and Locating (TTL) technologies and operations. Knowledgeable in the Army’s Operating Concept 2025, Expeditionary Mission Command Concept, and the Army’s Network 2020 and beyond and Network Convergence plans as well as the Cyber Electromagnetic Activities (CEMA) doctrine. In-depth understanding of the procedures and challenges of cross-platform interoperability and distributed data management operations in Joint, Interagency, Intergovernmental and Multinational (JIIM) environments. Expertise in the Department of Defense acquisition and budgetary processes.

CYBER SKILLS & EXPERIENCE

Knowledgeable in the principles of Cyber Operations including offensive, defensive and exploitation operations. Experienced in Cyber threat reconnaissance, scanning, exploitation, post exploitation, data exfiltration and persistent access attack-chain methodologies. Skilled in the identification of computer attacks as well as the preparation, identification, containment, eradication, recovery, and lessons learned cycle of incident handling. Skilled in the Active Cyber Defense cycle, Cyber Threat & Counter Intelligence operations, Social Engineering, Cyber deception principles, and evaluation of Intelligence successes and failures. Knowledgeable adversary modeling, data hiding techniques, cryptology, penetration testing and vulnerability assessments as well as the legal and ethical issues surrounding cyber operations.
EMPLOYMENT HISTORY

Jul 2016 – Present, University of Arizona – Director, Cyber Operations
Program Director for the Bachelors of Applied Science in Cyber Operations degree program. Reverse Engineered the Cyber Operations degree program, aligning program objectives with NSA knowledge units, and coordinated with the National Security Agency’s Cryptologic School to submit an application for the Center of Academic Excellence in Cyber Operations (CAE-CO) designation. Developed fifteen (15) new Cyber Operations courses, successfully obtaining curriculum committee approval and UA course catalog inclusion. Developed a Cyber Virtual Learning Environment, which includes a Virtual City, Malware Lab, Cellular system simulation (CellSim), Exploitation Lab, Forensics Lab, Capture the Flag Arena, Network Operations Center, and three (3) Internet of Things (IoT) Labs that directly support the learning objectives for the Cyber Operations degree program. Fostered a collaborative relationship between UA South, College of Engineering, Office of Research and Discovery (ORD) and the Eller Management Information Systems (MIS) Department for Cyber education and research programs. Established a relationship with DoD (AT&L) Cyber Models & Simulations Technical Working Group, National Cyber Range, and the Michigan Cyber Range. Developed two Offensive Cyber Operations (OCO) research programs, demonstrated advanced capabilities to NSA, OSD, CYBERCOM, ARCYBER, INSCOM, and DOJ representatives, and began discussions for technology transfer to the government. Developed and managed the solicitation, selection and execution of three software development and two construction contracts.

Developed company Cyber implementation strategies, staff professional development/training programs and direct Cyber program development efforts. Architected a segmented network integrating Threat Intelligence-driven Network Security Monitoring (NSM) and Threat and Environment Manipulation (TEM) techniques to allow for an active cyber defense paradigm to be adopted and implemented. Developed a Cyber-protected Secure Power Generation solution for Critical Infrastructure assets within the US Government. Designed a Cyber protection solution for Industrial Control and Combat Systems for a US Government requirement. Managed the design effort for the safety critical flight avionics and ground control station (GCS) for an advanced VTOL Unmanned Aerial System (UAS). Managed the transition of DOD technologies into the Oil & Gas industry to included turbine powered hydraulic fracturing units and island power generation units.

Developed focused solutions to produce immediate results for the Departments of Defense and Homeland Security. Working with DA G2, USAICOE leadership and subject matter experts, conducted a DOTML-PF+P assessment of the MI Rebalance, Relevant ISR to the Edge (RITE) and the Army & Intel 2020 plans identifying several critical gaps then developed solutions that were adopted by the Army to address those gaps. Led the analysis and design of the Vigilant Pursuit program. Developed the functional design for the SIGINT Pursuit (SPV) and HUMINT Pursuit Vehicles’ (HPV) Signals Intelligence, Cyber, Radar and Site Exploitation collection and exploitation
systems. Co-developed the Rapid Site Exploitation JCTD. Led the functional design of the SIGINT and Cyber exploitation capabilities and the integration of those technologies into DA G2’s QRC program supporting the Army’s Multifunctional teams. Developed the GEOINT Force Enhancement Module (FEM) and led the implementation of the system to support the mitigation of operational GEOINT PED shortfalls. Assisted in the design and development of the SensorWeb JCTD.

Aug 2002 – Feb 2009, Department of the Army - Director, Battle Command Battle Laboratory-Huachuca.
Directed and managed the Battle Command Battle Laboratory’s experimentation, models & simulation and prototyping programs in support of the US Army Intelligence proponent and the Training and Doctrine Command (TRADOC). Managed organizational and contract personnel and efforts spread across 43 locations within CONUS and 8 locations OCONUS. Managed the Battle Laboratory’s Joint Capabilities Integration and Development System (JCIDS) process and efforts, supporting all Intelligence program evaluations conducted by TRADOC. Developed and managed over 150 prototyping projects that directly addressed Combatant Command (COCOM) and Program of Record (POR) critical shortfalls. Developed and managed over 30 TRADOC experiments that spanned the breadth and depth of the Intelligence Warfighting function. Designed and managed the development of advanced Model & Simulations (M&S) tools in order to examine the current and future concepts, systems and organizations to the entity level of detail within both open and rolling terrain and complex urban environments. Managed the development and execution of over 300 development and support contract packages. Experienced in SOW/PWS/SOO/OTA development, project and program management, the Federal Acquisition Regulation (FAR) and Intellectual Property (IP) protection and management.

Served as the USAREUR Rapid Prototyping Officer. Managed the deployment and operations of multiple special purpose built SIGINT & Cyber exploitation systems in direct support of critical collection operations for Task Force Eagle, Task Force Falcon as well as several classified missions within the EUCOM theater of operations. Managed the deployment and operations of the first prototype Prophet systems in support of the Balkans Focus mission. Managed the deployment & training for the DragonEye and Pointer UAV systems for Task Force Eagle and Task Force Falcon.

Managed Intel activities and tasking for the 66th MI Group, V Corps and Special Mission Units supporting Operation Enduring Freedom, KFOR, SFOR and other classified missions supporting the Balkans Focus mission. Served as a rotational Deputy G2 for Task Force Falcon (TFF), Camp Bondsteel - Kosovo. Deployed the first civilian airborne ISR asset (AirsCan) to TFF. Managed the Intelligence section of the Joint Monthly Readiness Review (JMMR), and Integrated Priority List (IPL) sections and provided requirements input into the USAREUR POM and Commanders Narrative submissions for the USAREUR Commander. Managed the redeployment of the 1st MI BN (GRCS) move from Brindisi to Galatina, Italy in support of critical KFOR mission
requirements. Led the negotiation efforts with the Italian General Defense Staff in order to secure airbase use rights as well as coordinated both airspace and RF deconfliction.

May 1996- Oct 1999 – United States Army - Infantry Officer, 2-22IN, 10th Mountain Division, Fort Drum, NY.
Served as a Rifle platoon leader, Support platoon leader, HHC XO, and the Battalion S4 supporting both wartime and peacetime operations within the Balkans and Central America. Designed and managed 10th Mountain Division’s Lightfighter Academy Mission Readiness Exercise (MRX) in support of the Division’s Task Force Eagle - Bosnia deployments. Managed operational logistical support to the US Military Academy at West Point in support of cadet training. Conducted three rotations to the Jungle Operations Training Center (JOTC), Fort Sherman, Panama.

Extensive experience in enlisted leadership positions within the Infantry, LRS(D) and Special Operations communities.

EDUCATION

MS Cyber Operations 2016
MBA, Masters of Business Administration 2004
BA, Political Science 1996
Electrical Engineering 1993
SANS SEC 504, 560, 562, 567, 580, 617 2014-17

PUBLICATIONS

Attacking the Human – The Weakest Link in Cybersecurity 2016
CURRENT ROLE
Assistant Professor of Practice with the University of Arizona’s Cyber Operations department. Currently teaching Introduction to Network, Computer Investigations and Forensics, Introduction to Cyber Security, and Wireless Networking and Security.

Lead and manage a research team for the development of visualization capabilities for computer networks through virtual reality applications. This research will enhance the ability for cyber professionals and the National Security Agency to develop, refine, and rehearse offensive cyber operations in support of national directives.

RESEARCH AND GRANTS
Competed for and was received a total award of $423,723 from the NSA to conduct research into the utilization of Virtual Reality to support offensive cyber operations. Specifically, this will address the visualization of network traffic and net flow data to develop, rehearse, and refine cyber-attacks. Research will also be conducted on the feasibility and validity of using virtual reality to improve the comprehension and retention of information obtained by computer network traffic analysis. Additionally, I supervise the research team, which consists of one funded faculty member, two funded student researchers, one funded student work, and two student volunteers.

PROGRAM AND CURRICULUM DEVELOPMENT

CYBV 326 Introduction to Networking - Developed all course content to include: lectures, exercises, and assessments to comply with National Security Agency - Center of Academic Excellence in Cyber Operations designation requirements.

CYBV 388 Computer Forensics and Investigations - Developed all course content to include: lectures, exercises, and assessments to comply with National Security Agency - Center of Academic Excellence in Cyber Operations designation requirements.

INITIATIVES

Virtual Reality Research Lab - Designed, resourced, and implemented a lab environment to support research, interactive student engagement, industry partnerships, and a mechanism to increase the University’s stature within the local community, state of Arizona, peer institutions, and national partners.

The lab provides the following interdisciplinary capabilities:

Virtual Reality Equipment and Software
Digital Forensics equipment and software
Cyber/Network Security Tools
Internet of Things Devices for research
Security Fundamentals Workshop - Developed a 40-hour course on cyber security fundamentals, which will cover managing risk, monitoring and diagnosing networks, understanding technology devices and infrastructure, identity and access management, wireless network threats, securing the cloud, host, data, and application security, cryptography, threats, attacks, and vulnerabilities, social engineering and other foes, security administration, and disaster recovery and incident response. I will provide face-to-face instruction to students for this course.

SERVICE

Committee member for the interviewing and selection process for the Assistant Professor of Practice - Cyber Security Computer Scientist Position. Three faculty candidates came for campus visits, teaching demonstrations, and research proposals/demonstrations

Ongoing work with middle school students in the robotics program at Veritas Community Christian School to provide background and guidance for their robotics competition. Provided virtual reality experiences to allow students to better understand the International Space Station and the vastness and isolation in space. Review panel member for student research findings and interact students to increase knowledge within the STEM fields through guidance and mentorship.

EXPERIENCE

University of Arizona  Sierra Vista, Arizona  August 2018 – Present

Assistant Professor of Practice, Cyber Operations


Competed for and received an NSA research grant. Currently managing research into the development of a network visualization tool that will leverage virtual reality. This research will allow users to model threat networks and develop offensive cyber-attacks against traditional and software defined networks.

US Army  Sierra Vista, Arizona  August 2016 – September 2018

Project Manager, Requirements Determination Directorate, LandWarNet Chief

Manage eight personnel and ongoing projects involving communication and data systems for the Department of Defense (DoD). Analyzes and assesses intelligence and communications equipment for future development and integration into the DoD inventory. Provides relative insight to facilitate integration and development of products and procedures to support U. S. Policy and directives.

• Planned, managed, and executed multiple complex, multi-organizational events spanning three military branches representing 15 organizations and 20 geographical locations


Manager Information Technology

Managed 16 IT professionals that established, monitored, troubleshoot, and maintained voice and data networks for an organization consisting of 500 employees. Developed and sustained physical and network security measures. Provided mission analysis, project management, and training to employees for all IT aspects. Established and maintained health information system and the necessary training for
all health care providers. Programs utilized include but are not limited to Essentris, CHCS, AHLTA, HIPAA compliance.

- Solved complex problems with limited resources; for example, established a voice and data communication network to support 500 personnel with zero established infrastructure to support a hospital capable of treating up to 84 combat casualties. Resourced necessary supplies, equipment, and personnel to ensure that communications could be conducted with adjacent military and civilian agencies, including air and ground medical evacuation elements.

**US Army**  Colorado Springs, Colorado  June 2010 - July 2014
*Manager Information Technology*

Managed 11 IT professionals that established, monitored, troubleshooted, and maintained voice and data networks for an organization consisting of 310 employees. Additionally, developed and sustained physical and network security measures. Provided mission analysis, project management, and training to employees for all IT aspects.

Executive Officer of 70 personnel; ensuring the maintenance and accountability of $12 Million worth of equipment. Responsible for the administrative, training, and personnel actions for all personnel.

Operations Officer/Security Manager for six internationally dispersed companies responsible for maintaining 24-hour satellite communication operations for the Department of Defense.

**EDUCATION**

**Liberty University**  Lynchburg, VA
- Masters of Science Cyber Security

**Touro University International**  Cypress, California
- MBA Human Resources/Personnel Management

**Park University**  Parkville, Missouri
- Business Management Marketing
- Social Psychology

**SKILLS, CERTIFICATIONS, COURSES**

- Top Secret/Sensitive Compartmentalized Information (TS/SCI) Security Clearance
- Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), CompTIA Advanced Security Practitioner (CASP), Security +, Network +, A +
- Cyber Warfare/Penetration Testing Course / Active Cyber Defense Course (UA)
- Advanced Information Technology Management Course, Signal Captains Career Course (US Army)
- Basic Information Technology Management Course, Signal Officer Basic Course (US Army)
- Junior Management Training Course, Officer Candidate School (US Army)
- Senior, Advanced, and Basic US Army Leadership Course (US Army)
# Curriculum Vitae

## Thomas Jewkes

October, 29, 2018

## CONTACT INFORMATION

<table>
<thead>
<tr>
<th>Thomas Jewkes</th>
<th>Assistant Professor of Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Operations Program</td>
<td>The University of Arizona</td>
</tr>
<tr>
<td>An NSA designated Center of Academic Excellence in Cyber Operations (CAE-CO)</td>
<td>E-mail: <a href="mailto:tjewkes@email.arizona.edu">tjewkes@email.arizona.edu</a></td>
</tr>
<tr>
<td>Office: Room A115, Sierra Vista Campus</td>
<td></td>
</tr>
</tbody>
</table>

## RESEARCH INTERESTS

I’m interested in Active Cyber Defense and the design and implementation of Zero-Trust Networks.

## CERTIFICATIONS

- CompTIA Security+ CE 2017
- ITIL V3 Foundation Certificate in IT Service Management 2011
- Geomatics, Applied Mapping Sciences 2003

## SECURITY CLEARANCE

Top Secret/SSB

## EDUCATION

<table>
<thead>
<tr>
<th>University of Arizona South</th>
<th>August 2018 to Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistant Professor of Practice</td>
<td></td>
</tr>
<tr>
<td>Cyber Operations Program</td>
<td></td>
</tr>
</tbody>
</table>

At the University of Arizona, I have updated course material and taught in the Cyber Operations Program for the CYBV 301 Fundamentals of Cybersecurity, CYBV 385 Introduction to Cyber Operations, and CYBV 400 Active Cyber Defense courses.

<table>
<thead>
<tr>
<th>University of Arizona South</th>
<th>March 2017 to May 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjunct Professor</td>
<td></td>
</tr>
<tr>
<td>Cyber Operations Program</td>
<td></td>
</tr>
</tbody>
</table>

At the University of Arizona, I have developed and taught in the Cyber Operations Program for the CYBV 385 Introduction to Cyber Operations, and CYBV 400 Active Cyber Defense courses.

<table>
<thead>
<tr>
<th>American Systems</th>
<th>February 2013 to Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Analytics and Test Professional</td>
<td></td>
</tr>
</tbody>
</table>

I conducted cybersecurity conformance testing based on the Department of Defense (DoD) Information Assurance and Accreditation Process (DIACAP) and Risk Management Framework (RMF) processes. In connection with this, I participated in and provided technical support for developmental and operational testing of DoD Information Network (DoDIN) devices for interoperability to ensure protection against unauthorized activity and to assess vulnerabilities and threats. I participated in testing to ensure conformance with the DoD Instruction (DoDI) 8510.01 security control selection, monitoring, and remediation. Furthermore, I provided input and recommendations for future cybersecurity test activities.

| TASC                     | June 2006 to February 2013 |
Lead for Data Analytics

In support of the Ballistic Missile Defense System (BMDS) communications architecture, I traveled to remote test sites as an organization representative. I then collected and performed trend and pattern analyses of information exchanges. I maximized the efficiency and the organization of data analysis through use of improved analytical models and automation methods. The efforts included aggregating and reconciling data from various sources using Perl Compatible Regular Expressions (PCRE) for analyzing unstructured text-based data in Perl, JMP and R statistical software.

Subject Matter Expert

As the Subject Matter Expert in data analytics, I identified key datasets and data-sources. I initiated data mining procedures using Extract, Transform, and Load (ETL) principles, Structured Query Language (SQL)/Data Manipulation Language (DML) statements. The SQL/DML procedures included the use of aggregate functions, window functions, joining, ordering and grouping, and nested queries. To improve the analysis process, I enhanced data mining efforts using Entity Relationship Diagrams (ERD) to model database requirements, Microsoft SQL Server 2008 R2 (T-SQL), Microsoft SQL Server Analysis Services (SSAS), R statistical software, JMP 9, and Perl and PHP to improve pattern identification and anomaly detection.

Database Manager

As an ancillary responsibility, I managed multiple Microsoft SQL Server database instances. I coordinated database acquisition and analysis efforts with local and remote team members. I Interviewed users throughout the development cycle to improve usability of the end-product. I also prioritized and delivered products for multiple complex projects.

DynamicCity February 2005 to April 2006

Geospatial Analyst

The tasks for this effort were nearly exclusive to the geospatial analysis environment. The ability to adapt and the flexibility to think quickly, however, have translated to many other technical and non-technical fields.

At this company, I learned that others would come to me for help with technical issues. I quickly became a knowledge resource for others. I also learned that I enjoy showing others new approaches to old methods.

As a geospatial analyst working on a municipally-owned fiber-to-the-premise project, I performed highly-detailed geospatial data modeling and spatial ETL. I participated in field collection of real-world features using a Trimble Global Positioning System (GPS) unit. The Trimble allowed me to associate feature attributes such as locations and types of existing fiber optic cables, connection cabinets, telephone poles, and buildings. Moreover, I audited, validated, and analyzed data from complex and disparate sources. I created and updated personal geodatabases, in addition to versioned Arc Spatial Database Engine (SDE) geodatabases using expert knowledge of Geographic Information System (GIS) data warehouse concepts. Versioning responsibilities also included reconciling and posting versioned data to the data warehouse, thereby maintaining referential integrity.

Task Automation

In the office, I participated in data automation by expanding the functionality of the ArcGIS 9.3 software through the Visual Basic Editor. I produced customized soft- and hardcopy maps and data conversion of various formats. I also trained other ArcGIS users in troubleshooting and customizing the software.

I performed moderately complex SQL queries and various data modeling tasks included updating, querying, and exporting tables from a Relational Database Management System (RDBMS) (Oracle 9i). Many of the geospatial tasks involved highly technical and extremely detailed efforts. For example, I compressed and analyzed ArcSDE geodatabases using the command prompt; reconciled and posted versioned data; and performed data auditing and data correction.
### Team Leader

As the field team leader, I trained and motivated field data verification teams through daily technical and data verification briefings. I then coordinated with them throughout the day to complete set objectives. I provided daily task lists and instructed the teams relative to correct data verification methodologies.

### ReliaNet

**Business Relationship Manager**

As the business relationship manager, I communicated with end-users regarding their technology requests. I tracked their request status, delivery schedules, and facilitated communications with vendors. I participated in marketing strategy and development for current and future IT services.

### Field Technician

I participated in on-site design and management of the installation, configuration, and security of Wireless Local Area Networks (WLAN). I performed on-site analysis of physical layer network topology requirements and managed same-day installation for the customer. I interviewed customers to determine their current and future service needs. I provided on-site and remote technical support to the end-user. I participated in research and development of future IT strategies. I assisted with management of product inventory.

### Layton City Corporation

**GIS Technician**

As the intern, I produced customized soft- and hardcopy maps by digitizing existing paper maps using a digitizing tablet and heads-up digitization techniques. Once the maps were digitized and loaded into the database, I used the ArcGIS software to edit the variety of point, polyline, and polygon feature datasets representing the map features. I performed spatial data analysis by building ad-hoc SQL SELECT statements within the ArcGIS software. As I progressed, I learned to perform Spatial ETL for AutoCAD and raster and vector ArcSDE geodatabases. I also learned how to generate geometric networks representing traffic patterns. Gradually I began to expand the functionality of ArcGIS 8.3 through the Visual Basic Editor. I also began to explore web-based mapping with the ArcIMS software. At the time, the security of web servers at the city was not considered.

**Field Technician**

In an effort to improve and expand the offerings to the citizens of the community, I participated in field collection of land-use data for storage, edit, retrieval, and query. I participated in implementing new database products and technologies.

### VOLUNTEER

**CyberPatriot X**

Mentor for the 2017-2018; and 2018-2019 seasons. Provide training sessions to teach the students the fundamentals of identifying and mitigating system and network vulnerabilities in Windows desktop and server, Ubuntu Linux, and Cisco routers and switches.

### LANGUAGES

I am fluent in English. I also read and speak Spanish.
Dr. Elke Andrea Drennan  
2445 Isla Bonita Dr.  
Sierra Vista, AZ 85650  
Mobile: 520-508-1308  
Email: das.paar37@gmail.com

Work Experience:

**Carnegie Mellon University/Software Engineering Institute/CERT**  
Pittsburgh, PA  
Senior Engineering Liaison

Program lead for Cybersecurity training. Develop state-of-the-art, realistic Cybersecurity exercises for Department of Defense (DoD) cyber teams. Exercises are team-based, collaborative, and are developed in virtual environment. Incorporate standardized and virtualized tools and networks for training that is developed in accordance with DoD training objectives and guidelines. Participants actively operate, maintain, and defend their networks against realistic threats that consist of either live or pre-programmed injects.

Liaison/CMU representative to various DoD customers for multi-million dollar contracts. Responsible for gathering customer requirements and translating them into engineering tasks. Provide weekly updates to senior government representatives to report project status, identify potential risks, and address new customer requirements. Brief at the General Officer-level at least every quarter (more, if required). Oversee all projects and ensure that milestones are met and deliverables satisfy customer requirements. Manage project expenditures to ensure that projects are within budget. Work directly with SEI analysts and engineers in all departments to delegate work, address specific tasks, identify potential issues and risks, and ensure that the work stays aligned with customer requirements. Develop weekly and monthly project status reports. Perform scholarly research (in APA format) for DoD customers, as needed. Frequently collaborate with other universities and FFRDCs for expanded research projects.

**U.S. Army NETCOM G-6**  
Fort Huachuca, AZ  
08/2011- 03/2013

Information Management Branch Chief

As Information Management Chief for NETCOM, manage and coordinate all Information Management topics for NETCOM and its subordinate commands. Liaison to Army Cyber Command CIO/G-6, coordinating all activities, staffing actions, tasking subordinates, and gathering data to provide to higher headquarters. Manage the enterprise software license program for the entire command. Track licenses, gather requirements, and budget for current and future command-wide needs. Work with budgeting and accounting groups to obtain required funding. Develop Tactics, Techniques, and Procedures (TTPs) and Standard Operating Procedures (SOPs) to formalize processes and procedures for NETCOM. Manage and supervise government civilians; team lead for contractors. G-6 lead for Information Technology Asset Management (ITAM) capability.

**U.S. Army NETCOM G-5, Project, Plans and Architecture**  
Fort Huachuca, AZ  
10/2009- 08/2011

Capability Manager

IA team lead and Capability Manager for six LandWarNet Network (LWN) Operations (NetOps) capabilities: Secure Configuration Compliance Validation Initiative (REM/Retina), Situational Awareness and Risk Management, Network Access Control, Network Intrusion Protection Systems, Web Filtering/Proxy Management, and Assured Compliance Assessment Solution. Lead team of four contractors and two DA civilians to develop functional requirements documents, concept of operations, and detailed cost estimates to prepare and defend unfunded requirements. Oversee and direct projects’ implementation and sustainment efforts. Engage with higher commands and external organizations to coordinate efforts, share information, and gain project recognition. Coordinate with customers Army-wide (to include Tenants and Functional organizations) to ensure all organizations are incorporated into enterprise solutions. Prepare and defend project plans, technical reports, requirements packages, budget documents, formal communication, implementation guidance, and LOM acquisition documentation. Representative to the DoD Information Assurance/Computer Network Defense (IA/CND) Enterprise-wide
Solutions Steering Group (ESSG). Coordinate requirements within NETCOM/Army staff to ensure Army interests are properly represented.

U.S. Army Directorate of Information Management 11/2007-
Fort Hood, TX 11/2008

Systems Administrator
Perform system administration, analysis, design, development, and maintenance of various enterprise-level server applications and automated systems (Active Directory, Remedy, SMS (Systems Management Server), iLo) as well as network monitoring software (What's Up) (WUPP) and systems monitoring applications (Microsoft Operations Manager (MOM)), SANs, databases (SQL) and web services. As lead administrator, maintain, develop, and troubleshoot BMC Remedy. Create custom forms, views, menus, and actions, as required by the organization. Create and manage user accounts. Administer back-end SQL database, checking for errors, manipulating data, and performing back-ups as necessary. Prepare documentation for installations, configurations, and customizations of applications. Configured MOM and WUPP alerts to work with Remedy for automatic ticket creation. Integrated IT Metrics into custom Remedy menus to automate reporting procedures. Develop and propose changes for improvement to applications, configurations, databases, and web services in conjunction with IA policies and standards. Administer WUPP, compress and back-up database weekly. Utilize SMS remote tools and HP's iLO to remotely manage and troubleshoot systems. Administer iLO: create and manage user accounts and remote features. Utilize ADSI (Active Directory Services Interface) Edit and ADUC (Active Directory Users and Computers) to manage and configure user domain accounts, mailbox and distribution groups. Perform weekly Retina scans to ensure all devices are patched to meet IAVA compliance; patch devices as necessary. Post Web site updates for all units on installation. Volunteered to assist in ArcSight installation and configuration for Fort Hood. Provided technical feasibility guidance and general technical knowledge. Helped create organizationally useful connectors and output data. Assisted team members in the configuration of the database, manager, and console. Created custom filters for monitoring network/server/IDS events. Interact with coworkers and customers daily, working tickets, troubleshooting software applications, and sharing knowledge. Readily help coworkers whenever necessary and on own accord. Follow-through on projects started and volunteer for new responsibilities whenever possible.

U.S. Army European Theater Network Operations and Security Center 10/2005-
Mannheim, Germany 11/2007

Network Analyst

U.S. Army European Theater Network Operations and Security Center 11/2004-
Mannheim, Germany 10/2005

Systems Administrator
Responsible for managing daily operations and functions of servers, workstations, and thin clients in an environment requiring 24/7 availability, supporting theater-wide network management. Manage application servers in the E-TNOSC theater responsible for the network, performance monitoring, and problem reporting. Design system configurations and common user environments and interfaces. Perform Tier III troubleshooting for LAN problems, coordinating maintenance
requirements for E-TNOSC LAN. Serve as the IMO for the E-TNOSC division. Provide support to external agencies as required in support of E-TNOSC goals and objectives. Apply patches, upgrades, and AV configurations to manage inherent threats to systems. Oversee and perform maintenance to all assigned automation resources. Planned, coordinated, and prepared organization for migration to Active Directory (LWN-C). Streamline and standardize IT operations within the organization. Coordinate with local German organizations for equipment repair and part ordering/replacement. Interact/communicate with customers on a daily basis, both orally and in writing.

**U.S. Army RCERT-E/IAPM**
Mannheim, Germany
01/2004-11/2004

**Systems Administrator**
Primary Systems Administrator in support of the RCERT-Europe and the Office of the IAPM, USAREUR. Managed all Intrusion Detection Systems (both hardware and software) for the theater. Built and managed 2003 Advanced Server systems, including Web servers, and 2000 and XP desktops/laptops, classified and unclassified, troubleshooting and patching/maintaining all systems to meet IAVA compliance. Liaison to IMO, coordinating all organizational activities to include upgrades, software management, and user problems. Tested and implemented hardware and software for improved security management and remote control of critical theater resources. Documented all testing and system configurations to create a standard and for continuity. IASO for both organizations.

**U.S. Army Corps of Engineers**
Albuquerque, NM
09/2002-01/2004

**IT Specialist**
Install, configure, maintain, and troubleshoot network including hardware (servers, hubs, switches, and routers) and relevant software, locally and in field offices. Administer print and file servers (including WINS, DNS, Dcs). Very knowledgeable with desktop troubleshooting, currently supporting over 500 computers, remotely and locally. Test, install, configure, and troubleshoot hardware and software on clients and servers to ensure availability and functionality of systems. Analyze interrelationships of computer system components to determine possible causes and solutions to problems. Analytical and self-directed to independently diagnose and solve problems or to contribute to a team effort to find most effective solution. Task-oriented and decisive, either independently or in a team environment. Eagerly seek new challenges and responsibilities to increase expertise and skills in information systems architecture. Flexible nature enables functioning well in a fast-paced, ambiguous environment. Responsible for segments of IT projects, ensuring they meet time and budget constraints by planning sequence of actions to accomplish the mission. Coordinate with other team members to ensure task completion and to meet project milestones, adapting guidelines and precedents to the needs of the assignment. Organize and conduct user groups to facilitate information exchange and disseminate IM policies, procedures, and standards issued by higher headquarters.

**U.S. Army Corps of Engineers**
Kabul, Afghanistan
05/2003-09/2003

**Systems Administrator**
Sole IT support, IASO, and LAN/WAN administrator for USACE in Kabul, Afghanistan. Responsible for managing, maintaining, and troubleshooting all servers, including Microsoft Exchange mail server, network equipment, desktop PCs, laptops, and miscellaneous IT equipment (e.g., printers, copiers, phones). Planned, designed, developed, implemented, analyzed, and troubleshoot new and existing network configurations. Made and laid CAT 5 cables, configured switches and routers, performed testing and integrated hardware/software for full operability, functionality, and efficiency. Troubleshot all software/hardware problems on a daily basis and applied updates for optimal performance. Monitored for security threats, applied necessary patches, and prepared emergency backup plan. Identified and reported vulnerabilities to appropriate authorities and implemented corrective measures. Strategically planned to overcome possible IT failures to avoid downtime. Procured new/backup equipment to ensure day-to-day functionality and planned for expansion while minimizing costs. Coordinated with external Army organizations to maintain standards and enhance security. Configured, set-up, and maintained secure/classified video teleconferences on a weekly basis. Tested, maintained, and troubleshoot new systems including phones with VoIP functionality/configuration. Prepared to implement Active Directory on servers. Volunteered to create/design Web site for Afghanistan Area Office.
**U.S. Army Corps of Engineers**  
Albuquerque, NM  
09/2001-09/2002

**Computer Specialist**

Troubleshoot all types of hardware and software problems on desktops and servers. Advise customers, recommending hardware and software to fulfill user-specific requirements. Train users on new systems and build customized solutions to optimize their performance. Provide technical support and assistance on both hardware and software. Communicate with groups and individuals to solve general and specific problems. Acquire necessary software and hardware or provide vendor quotes when necessary. Very customer-oriented and personable. Highly analytical, breaking down problems to find most effective solution. Alternate Webmaster for district intranet. Design page layouts using Front Page and HTML 4. Test links, format site-content, and monitor data for accuracy.

**Education:**


M.A. in Computer Information Systems, Webster University.
B.S. in Business and Management and Psychology, University of Maryland.

4.0 GPA for all degrees.

Certified in ITIL v3, Security+, and Mac OS X Snow Leopard.

**Job Related Training:**

Java Programming (3 s.h.); Python Programming (80 hrs.); Army Management Staff College (120 hrs.); CCNA Bootcamp (40 hrs.); Certified Ethical Hacker (40 hrs.); CISSP (40 hrs.); ACQ 201A Intermediate Systems Acquisition Course (40 hrs.); Basic SQL (40 hrs.); ArcSight Certified Security Analyst (80 hrs.); Army Retina Scanner Virtual Training Course; Metropolis Wavelength Services Manager (WSM) (40 hrs.); Navis Optical Management System (OMS) (40 hrs.); Cisco: 7600 Series Essentials (40 hrs.); Cisco: Building Core Networks (40 hrs.); Blue Coat Professional/Administrator (40 hrs.); McAfee IPS (24 hrs.); Fundamentals of Systems Acquisitions Management (2.5 CEUs); Knowledge Management (40 hrs.); Secure Configuration Remediation Initiative (40 hrs.); Action Officer Development Course (21 hrs.); Supervisor Development Course (39 hrs.); Managing and Maintaining a Microsoft Windows Server 2003 Environment (OU Admin) (40 hrs.); Information Assurance Policy and Technology (10 hrs.); Microsoft 2282A (40 hrs.); Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure(40 hrs.); Intro to Cisco Networks (40 hrs.); Information Assurance Computer Network Defense II (40 hrs.); Information Assurance Computer Network Defense I (40 hrs.); Microsoft Desktop Deployment (16 hrs.); Information Assurance Program (8 hrs.); Applying Desktop Security Baselines (8 hrs.); 2151 Microsoft Windows 2000 Network Operating System Essentials (40 hrs.); 2152 Implementing Windows 2000 Professional Server(40 hrs.); A+ Core Hardware Operating Systems (54 hrs.); Network+ (40 hrs.); Intern Leadership Development Course (ILDC) (40 hrs.); Customer Service Excellence (8 hrs.); Unicenter TNG (32 hrs.); HTML4 (32 hrs.); Dreamweaver (16 hrs.); FrontPage 2000 (16 hrs.); Project Programming (USAF) (80 hrs.)

**References:**

COL Charles Wells, Retired, PM, DCGS-A, (703) 634-9885; charles_wells@symantec.com  
Mr. Earl Pray, Deputy IAPM, +49 176-42913415; earlbert56@gmail.com

**Additional Information:**


AFCEA board member.

Award - Recognition for Volunteering in Afghanistan (08/22/2003)  
Commended for service provided to U.S. government while deployed.

Award - Commander's Awards for Civilian Service (08/04/2003)  
Recognized for excellent service provided to the U.S. Army.

Speak, read, and write German fluently and am proficient in Spanish.

Experienced with the following Remedy products: ITSM 7.0, Mid-Tier, Requester Console, Asset Management, and Data Management. Knowledgeable in server and desktop (software and
hardware) troubleshooting. Skilled with Cisco Works, Cisco Secure, Spectrum, IronView Network Manager, Citrix, UNIX, and various Oracle and third-party software. Communicate well with customers, internal and external, to find best solutions to IT problems. Thoroughly familiar with TCP/IP, OSI Model, LAN/WAN design principles, methodologies, and approaches used in developing, testing, installing, operating, managing, and maintaining network services that support functional requirements. Knowledgeable of network architecture, topology, protocols, and security requirements. Work well in team and/or individual environment. Honest, forthright, and organized.
Harry R Cooper  
747 Darley Green Drive, Claymont, DE 19703  
315-266-7087  
harry@twcsec.com

Summary

- A cybersecurity technology professional with a track record of building and developing successful methods to carry out each assignment.

- Hold Master’s Degree in Cybersecurity, Intelligence and Forensics and Bachelor’s Degree in Political Science and in Spring 2018 a Doctorate in Cybersecurity.

- Experienced in the intricacies of computers and mobile devices in use today and yesterday. Additionally, experienced with the various ways and methods of using the Internet to carry out one’s actions and the interaction of said systems to businesses, public infrastructure, and other key areas. Experience ranges from technical support through cybersecurity development and implementation.

- Dedicated to enthusiastic and dynamic collaboration as a means of creating and nurturing successful projects to completion.

Education

<table>
<thead>
<tr>
<th>Degree</th>
<th>Institution</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctor of Science in Cybersecurity</td>
<td>Capitol Technology University</td>
<td>2018</td>
</tr>
<tr>
<td>Master’s Degree in Cybersecurity Intelligence and Forensics</td>
<td>Utica College, Utica, NY</td>
<td>2013</td>
</tr>
<tr>
<td>B.A. Degree in Political Science</td>
<td>University of Pittsburgh</td>
<td>2000</td>
</tr>
</tbody>
</table>

Research Work

<table>
<thead>
<tr>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of Information in the Age of Terrorism: The Mosaic Theory in Practice (Doctoral Dissertation)</td>
<td>2018</td>
</tr>
<tr>
<td>Attacking San Francisco’s Critical Infrastructure (A Cyber Threat Analysis) (Master’s Capstone)</td>
<td>2013</td>
</tr>
<tr>
<td>Latest Techniques for Cheating (Currently a workshop, but developing into a journal article)</td>
<td>2016-present</td>
</tr>
<tr>
<td>DarkWeb: Using Tor to safely surf the DarkWeb (Chapter in upcoming textbook from Taylor &amp; Francis/Routledge, Payment Systems in Fraud and Money Laundering Investigations)</td>
<td>2017</td>
</tr>
<tr>
<td>Peer Reviewer for The Journal of Digital Forensics, Security and Law</td>
<td>2016-present</td>
</tr>
</tbody>
</table>

Career History & Accomplishments

**Adjunct Instructor, Capitol Technology University**  
2017 - present

- Taught courses at the Undergraduate level.
- Courses taught include:  
  - Intro to Cyber Network Operations

**Adjunct Instructor, Southern New Hampshire University**  
2015 - present

- Taught courses at the Graduate level.
- Courses taught include:  
  - Incident Detection and Response Investigations - Digital Forensics  
  - Core Technologies  
  - Security Risk Analysis and Planning
Cyberlaw and Ethics

**Adjunct Instructor**, *Wilmington University*  
- Taught and re-developed courses at the Graduate level.  
- Courses taught include:  
  - Operating System and Computer Systems Security  
  - Web and Data Security  
  - SCADA Architecture  
  - SCADA Risk Management and Auditing  
  - Business Intelligence  
  - Action Research Fieldwork  
  - Field Experience/Internship

**Professor of Practice**, *Utica College*  
- Taught and re-developed courses at both the Graduate and Undergraduate level.  
- Courses taught and re-developed during this period include:  
  - Foundations of Computing for Cybersecurity  
  - Principles of Cybersecurity  
  - Cyber Counterintelligence  
  - Cybercrime Investigations and Forensics II  
  - Systems Vulnerability Assessments  
  - Information System Threats, Attacks and Defenses  
  - Network Forensics  
  - Cyber Intelligence  
  - Critical National Infrastructures and National Security  
  - Tactics, Techniques, and Procedures  
  - Principles of Cybercrime Investigations  
  - Computer Hardware and Peripherals  
  - Computer Network Investigations

**CEO/Partner**, *Thimbleweed Consulting and TWC Security*  
- Held key responsibility in this company for not only running the day to day aspects of the company but also handled the role of being one of its principals.  
- Successfully led the development of a free open source Forensic tool called All-In-USB.  
- Worked on multiple projects encompassing everything from simple websites to more complex projects such as a resource scheduling system for a light manufacturing company that runs their entire facility.  
- Personally handled almost all security related projects from simple website defacements to a case involving the online slandering of a nationally recognized football team.  
- Developed a new hardware keylogger chip for use by corporate and government groups.  
- Developing a series of mini computers that can be used for everything from network monitoring to penetration testing to battlefield forensics.

**Computer Skills**  
- **Languages:** HTML, CSS, DHTML, Javascript, VBScript, ASP, Visual Basic, PERL, Visual FoxPro, MySQL, PHP, ColdFusion, and more.  
• **Software:** Adobe Photoshop, Adobe Illustrator, Adobe Pagemaker, Pervasive's Tango, R:Base (a relational DBMS), Microsoft Office Family, Microsoft Outlook, Site Server Commerce, Microsoft’s Internet Information Services, Microsoft Visual InterDev, Apache Web Server, Navision Financials, QuickBooks, NetSuite, Digital Photography Studio, Adobe Master Collection, Ariba (EDI), Microsoft Exchange Administration, Oracle (using NetSuite Development Tools), and other educational and commercial packages. CMS experience with Joomla and variants.

• **Intelligence and Forensic Software and Hardware Experience:** Developed the open source package All-in-USB forensics tool suite. Software packages used include FTK, DEFT Linux, CAINE, IDA, REMnux, Maltego, mdd, Volatility, Helix3, VMWare, Gephi, DFF, and many more.
Mohamed Meky
3616 Turkey Path Bnd
Cedar Park, TX 78613, USA
(732) 533-8250
mmeky@arizona.edu

SUMMARY
A professional who has a unique combination of teaching, research, and industrial experiences. I have more than 20 years teaching experiences in EE, IT, CS, and Cyber security programs. I have taught several security courses including cybersecurity, Malware analysis, Secure Software Development, Operating Systems, C-programming, Assembly language, UNIX, networking, system administration, computer language programming, and other technology courses. As a cyber security subject matter expert, I developed several courses in cyber security area for several graduate and undergraduate cyber security programs.

EDUCATION
Ph.D. in Electrical Engineering, City University of New York, GPA 4/4, 05/93-02/98
Dissertation: "Objective Evaluation of Speech Quality over Telecommunication Networks using Neural Networks"

M.Sc. in Electrical Engineering, Alexandria University, Egypt, GPA 3.9/4, 09/87-10/90
Thesis: “Semiconductor Lasers for Optical Communication”

B.Sc. in Electrical Engineering, Alexandria University, Egypt, GPA 3.9/4, 09/83-07/87
Distinction with Honor Degree, top of the Class (280 students)
Project: “Very Large Scale Integrated (VLSI) Circuit Design”

CYBER SECURITY CERTIFICATE
Foundations of Cyber Security Certificate, University of Maryland University College (UMUC), USA, Nov. 2011

ONLINE TEACHING CERTIFICATES
• American intercontinental University faculty certified facilitator, USA, 2010
• University of Maryland University College (UMUC) faculty certified facilitator, USA, 2010
• Regis University faculty certified facilitator, USA, August 2009
• University of Bellevue faculty certified facilitator, USA, 2008
• Florida Institute of Technology faculty certified facilitator, USA, 2007

SUBJECT MATTER EXPERT (SME)
• Western Governors University (WGU), USA, 10/2015-12/31/2016
  Review the content and recommend additional learning resources for the following cybersecurity courses:
  • Cyber warfare
  • Secure Network Design
  • Secure Software Design

• Thomas Edison State University, New Jersey, USA 06/2017- 10/30/2017
  Develop the following cybersecurity course:
  • Ethical Hacking

TEACHING CYBER SECURITY COURSES
02/2017-Present
NSA designated Cyber Operations program, University of Arizona, Arizona, USA
• CYBY 454- Malware Threats and Analysis

08/2012-Present
MS in Information Assurance and Cybersecurity, Florida Institute of Technology, Florida, USA
• SWE 5660 – Secure Software Development
• CYB 5665 – Secure Web Services
• CYB 5288 – Computer-Organization-and-Architecture
• CYB 5275 – Enterprise Information Security
• CYB 5277 – Computer and Information Security
08/2011-Present
Master in Cyber Security, Bellevue University, Nebraska, USA
- CYBR 420 – Cyber Investigation & Forensics
- CYBR 410 – Database Security
- CYBR 525 – Ethical Hacking and Response
- CYBR 515 – Security Arch & Design,
- CYBR 608 – Information Security Management
- CYBR 625 – Business Continuity and Recovery Planning
- CIS 313 – Cryptography

03/2016-Present
Master in Information Security, DeVry University, Texas, USA
- SEC 572 – Network Security
- SEC 572 - Ethical Hacking
- SEC 280- Principles Info Sys Security

08/2012-12/2013
Cyber Security Certificate Program, University of Colorado, Global Campus, USA
- ISM531- Cyber Security Defense and Countermeasures,
- ISM529- Emerging Cyber Security Technology Threats and Defense
- ISM530 – Enterprise Security
- ISM527- Cybersecurity Management
- ITS425– Ethical Hacking and Penetration Testing
- ITS360 – Introduction to Cyber Security and Digital Crime

OTHER COURSES TEACHING EXPERIENCE
- C/C++ Programming Courses,
  Rigs University, CD Dept., Colorado, USA, 2013-2014
  NY City Technical College, CS Dept., Brooklyn, USA, 1995-1997

- Data and Networking Courses
  Rigs University, 2013-2014
  Florida Institute of Technology, 2008-2011
  Bellevue University, 2008-2011

- Unix/OS/Database Courses (14 different IT courses)
  Bellevue University, 2008-2011

- EE/Telecommunication Courses
  City University of New York, 1993-1998
  Alexandria University, Egypt, 1997-1993

OTHER ACADEMIC EXPERIENCE
1- Developing New IT Courses
- Developing a wireless communication course (CIS5400) for Master of Science (Information Technology), Florida Institute of Technology, 05/07 – 08/07
- Developing a data networking course (CIS5410) for Master of Science (Information Technology), Florida Institute of Technology, 09/07 – 01/08
- Developing a UNIX administrator course (CIS5530) for Master of Science (Information Technology), Florida Institute of Technology, 05/08 – 08/08
- Developing a network security course (CIS5420) for Master of Science (Information Technology), Florida Institute of Technology, 09/08 – 01/09

2- On Campus Teaching Program
- Teaching/Research Assistant, City University of New York, EE Dept., NY, USA, 05/93-07/96
  Electronics, wireless communications, and computer communications courses
- Adjunct Professor, Manhattan College, CS Dept., New York, USA, 09/93-05/96
Digital Design Switching System, and Circuit Linear System I, and II courses

- Adjunct Professor, **NY City Technical College**, CS Dept., Brooklyn, USA, **01/95-12/97**
  C++ Programming I, and II courses

- Adjunct Professor, **LaGuardia College**, CS Dept., Queens, USA, **01/96-05/96**
  Electronic Circuit I, and Computer Repair courses

**3- Teaching Abroad**

- Assistant Professor, **Faculty of Eng.**, EE Dept., Alexandria, Egypt, **07/01-03/02**
  Telecommunications and Microwave Electronics Courses

- Teaching/Research Assistant, **Faculty of Eng.**, EE Dept., Alexandria, Egypt, **09/88-05/93**
  Electronic Circuits, Theory of Communication Engineering, Digital Computers, and Automatic Control

**INDUSTRIAL EXPERIENCE**

**InfoCom Technology Inc**, Paterson, New Jersey, USA, **8/00-12/2014**
(Consultant)
Implementing, designing and testing telecommunication services.

**NYNEX Science& Technology**, White Plains, New York, USA, **6/96-11/97**
(Consultant)
Research, developing, and designing of new speech & video compression and measuring its transmission quality over digital network such as ISDN, and Internet.

**City University of New York**, Multimedia Lab, New York, USA, **5/93- 6/96**
(Research Assistant)
Research/developing and designing of new objective techniques that used to predict the Quality of Services over Telecommunication networks

**PROFESSIONAL ACTIVITIES AND ACHIEVEMENTS**

- Co-author of the book “Freshman Course in Electrical Engineering ENGR. 103,” Electrical Engineering Department, City University of New York, 1996

- Invited referee for the **IEEE Journal on Selected Areas in Communications (JSAC)**, 1996.

- Invited referee for the **Second IEEE Symposium on Computers and Communications (ISCC’97)**, Alexandria, Egypt.


- Invited referee for the **Fourth IEEE Symposium on Computers and Communications (ISCC’99)**, Alexandria, Egypt

- Member, **IEEE Communication Society**

- Member, **IEEE Reliability Society**

- Member, **DSL Forum**

**AWARD**

- “Graduate Research Assistantship,” Research Foundation of the City University of New York, 1993-1996

- “Graduate Teaching Assistantship,” EE department, City College, City University of NY, 1993-1996


**RESEARCH AREAS**

- Cyber Security
- Cloud Computing
- Speech quality Algorithms
- Wireless communication

---

1 Changed to Verizon
PUBLICATIONS

Journal Papers


Conference Papers


Books


Internal Memorandums


SEMINARS AND INDUSTRIAL TRAINING


3- **M. Meky**, “Objective Evaluation of Speech Quality” *A seminar given for AT&T Voice Services Division, Middletown, New Jersey*, Nov., 2000

4- **M. Meky**, “ISDN Protocol Analyzer,” *A training session given for AT&T Performance Group, Middletown, New Jersey*, June 1999

5- **M. Meky**, “Objective Evaluation of Speech Quality Over ATM Networks Using Neural Networks” *A seminar given for AT&T ATM, and Wireless Stakeholder, Middletown, New Jersey*, April, 1998

---
2This paper has been selected for Best Paper Category
HEIDI A. CALHOUN-LOPEZ

FORMAL EDUCATION

U.S. Army Special Victim Counsel Course, Charlottesville, Virginia January 2018

U.S. Army Command and General Staff Officer Course May 2017

U.S. Army Judge Advocate Officer Advanced Course, Charlottesville, Virginia January 2013

U.S. Army Judge Advocate Tactical Staff Officer Course October 2011

U.S. Army Basic Instructor Course, Fort Huachuca, Arizona September 2008

U.S. Army Judge Advocate Officer Basic Course, Charlottesville, Virginia December 2005

Wake Forest University School of Law, Winston-Salem, North Carolina Juris Doctor May 1998

Duke University, Durham, North Carolina Bachelor of Arts, cum laude, Comparative Studies and Spanish May 1995

EXPERIENCE

United States Army Reserve 214th Legal Operations Detachment, Fort Snelling, Minnesota Legal Advisor, Special Victim Counsel October 2017 – Present

Currently serving as legal advisor and Special Victim Counsel for U.S. Army Reserve detachment. Spearheaded initiative to collaborate with the Armed Forces of Colombia to revise policies and procedures to reduce incidents of sexual assault and sexual harassment within Armed Forces of Colombia ranks. Selected by United States Army South to engage with leaders of Armed Forces of Colombia and to draft written assessment and recommendations directed at revising policies and procedures within Armed Forces of Colombia. Work recognized by as significantly impacting one of hemisphere’s key strategic partners. Earned the Army Achievement Medal.

United States Army Intelligence Center and School, Fort Huachuca, Arizona Instructor April 2008 – September 2009; July 2014 – October 2017

Served as legal instructor for the Army Intelligence Center and School. Responsible for teaching operational and intelligence law in 22 courses for over 6,000 students across the Department of Defense. Instructed students at all levels, to include senior commanders, company grade officers, NCOs, and junior enlisted servicemembers. Developed course curricula by integrating CENTCOM guidance, Law of Armed Conflict, and rules of engagement. Recognized by the Staff Judge Advocate for development of course of study for the Human Intelligence Legal Principles Course. Selected by SOUTHCOM to serve as member of a team tasked to train Colombian Armed Forces members on operational law matters in Cali, Colombia (in Spanish); recognized by the Commanding General of United States Army South for “outstanding support.” Earned the Meritorious Service Medal.

United States Southern Command, Doral, Florida Legal Advisor July 2011 – July 2014

Served as Assistant Staff Judge Advocate in Drilling Individual Mobilization Augmentee (DIMA) status. Provided legal advice and support to the Commander, U.S. Southern Command, the Army Element Commander, the Headquarters staff, and 32 Security Assistance Offices in the area of responsibility. Primary topics included international law and the law of armed conflict. Engaged in military to military relations with Central and South American counterparts both at SOUTHCOM and in Central and South America using fluent Spanish skills. Selected by Defense Institute of International Legal Studies to serve as instructor (in Spanish) at Naval Small Craft Instruction and Technical Training School (NAVSCIATTS) for law of armed conflict course for officers and enlisted members of militaries of Guatemala, Honduras, and Peru; recognized by NAVSCIATTS commander for outstanding teaching and support. Selected to serve as Victim-Witness Liaison (VWL) in criminal actions
throughout SOUTHCOM area of responsibility; traveled to Medellin, Colombia as VWL in connection with high profile courts martial arising out of misconduct at Summit of the Americas (Cartagena, Colombia). Selected to travel to Guantanamo Bay (GTMO) as part of SOUTHCOM quarterly inspection team to ensure compliance with detention law and policy. Voluntarily mobilized to GTMO on 90 day orders to serve as legal advisor to investigating officer appointed to investigate detainee death at detention facility; recognized for contributions leading to a “timely and impressive” report approved by the Combatant Commander. Earned the Joint Service Achievement Medal.

Office of the Staff Judge Advocate, Fort Hood, Texas and Camp Liberty, Iraq
Administrative and Fiscal Law Attorney

April 2007 – April 2008

Served as administrative and fiscal law attorney for the 1st Cavalry Division, a unit of over 19,000 servicemembers. Advised the command on all issues related to federal and state laws and Army regulations, including fiscal law, ethics, and command oversight. Coordinated administrative investigations, including investigations into violations of the law of war and rules of engagement, and sensitive investigations into senior-officer misconduct. Advised judicial officers in summary courts-martial and investigating officers in pretrial hearings to determine probable cause to proceed to trial. Served as a Military Magistrate to authorize search warrants and pretrial confinement. Earned the Army Commendation Medal.

Office of the Staff Judge Advocate, Fort Hood, Texas and Camp Liberty, Iraq
Chief of Detainee Operations, Operational Law Attorney

April 2006 – April 2007

Served as primary detainee operations legal advisor to the SJA, Division Provost Marshal, Division G3, Division G2, and other staff members of a multi-national division consisting of nine maneuver brigade combat teams and four support brigades with almost 40,000 Soldiers on 19 forward operating bases. Oversaw legal aspects of detainee operations, including coordination with tactical ground units at the point of capture, detention at Brigade and Division-level facilities, and theater-level prosecution. Responsible for bi-weekly briefings to the Division Deputy Commanding General (Support) regarding legal aspects of detainee operations, including capture, processing, interrogation, and housing. Reviewed over 3,000 cases of detainees prior to referral to Theater Internment Facilities. Developed a Sensitive Site Exploitation Seminar and taught it to deploying units in garrison and to combat brigades in theater. Inspected each of the division’s seven detainee facilities monthly for compliance with law and policy. Advised the division’s targeting cell to ensure deliberate targeting operations complied with the Law of Armed Conflict. Earned the Bronze Star Medal and Army Achievement Medal.

Office of the Staff Judge Advocate, Fort Hood, Texas
Legal Assistance Attorney

2005-April 2006

Served as legal advisor to Soldiers within the Division. Advised clients on issues involving family law, landlord / tenant law, military administrative actions, consumer law, estate planning, and military benefits.

Astigarraga Davis, Miami, Florida
Attorney

September 2005

Represented financial institutions and multinational corporations in international civil and criminal litigation in North and Latin America. Represented United States financial institution and Argentine securities firm in suit brought in Florida court by investors alleging securities fraud; represented Fortune 50 multinational corporation in suit brought in federal court by Peruvian distributor alleging fraud, conspiracy, and antitrust violations. Drafted legal pleadings and memoranda, including motions to dismiss for forum non conveniens, lack of personal jurisdiction, and insufficient service of process, under United States and foreign law; participated in hearings and depositions; consulted on legal pleadings and memoranda in Spanish language based on foreign law in proceedings in foreign courts; prepared witnesses for hearings and trial in United States and foreign courts; investigated factual background of cases, often through travel abroad to interview witnesses and analyze documents. Traveled extensively throughout Europe and Latin America, including Mexico, Argentina, Chile, Ecuador, Peru (debrieved witnesses and strategized with local counsel to prepare for meetings with Peruvian prosecutors, re facts subject of criminal case in Peru against corporate client), and Trinidad and Tobago (met with Trinidadian government to advise on recovery of assets misappropriated in course of construction of Port of Spain airport).

Law Offices of Roy Black, Miami, Florida
Attorney

August 1999 – April 2001

4824 Lamplighters Lane • Minnetonka, Minnesota 55345 • (305) 975-5133 • heidi.calhounlopez@me.com
Represented criminal defendants, from grand jury investigation and indictment through trial, sentencing, and appeal. Defended clients in criminal cases in state and federal courts in United States, including the District of Puerto Rico, charged with: theft from a program receiving federal funds (18 U.S.C. §666); money laundering (18 U.S.C. §1956); transportation of stolen goods (18 U.S.C. §2314); importation of a controlled substance (18 U.S.C. §952). Drafted pre-trial motions, including motions to dismiss based on lack of federal jurisdiction and failure to indict within statute of limitations; assisted in formulating trial strategy; organized trial exhibits; prepared cross-examination of government witnesses; supervised government agency debriefings, and handled sentencing matters. Relocated to San Juan, Puerto Rico for several weeks to analyze documents, interview witnesses, and formulate defense strategy; acted as second chair defense counsel in month-long criminal trial in United States Federal District Court for the District of Puerto Rico involving allegations of conspiracy and theft in the provision of health services.

BAR ADMISSION
Florida, 1999

SPECIAL SKILLS
Top Secret Security Clearance
Fluent in Spanish (achieved top score 3/3 on Defense Language Proficiency Test, April 2014)
Qualified Collateral Damage Estimate Analyst

PUBLICATIONS AND SPEECHES
Speaker, “The Use of Foreign Criminal Proceedings as a Litigation Tool: Fair Game or Not?” Second Annual International Litigation Update, International Litigation and Arbitration Committee of the International Law Section of the Florida Bar, June 24, 2004

SIGNIFICANT AWARDS
Bronze Star Medal—awarded for service in Iraq as Chief of Detainee Operations
Meritorious Service Medal—awarded for service as Senior Legal Instructor
Army Commendation Medal—awarded for service as Administrative and Fiscal Law Attorney
Joint Service Achievement Medal—awarded for service at GTMO as Legal Advisor
Army Achievement Medal—awarded for service as Operational Law Attorney and as Legal Advisor
Combat Action Badge—awarded for active engagement with the enemy during combat service in Iraq

INTERESTS
Downhill skiing (NASTAR National Gold Division Qualifier, 2014; Ski Challenge League Competitor, 2013-2014)
Early childhood education (President, Parents’ Committee, Mundo Montessori, Laredo, TX 2011-2012; Trained Substitute Teacher, Mayflower Montessori, Minneapolis, MN 2013-2015)

REFERENCES
Colonel Daniel J. Lecce, USMC, Staff Judge Advocate, United States Southern Command
daniel.j.lecce.mil@mail.mil

Lieutenant Colonel Luis O. Rodriguez, USA, Deputy, Personnel, Plans and Training Office
luis.o.rodriguez12.mil@mail.mil
Attorney at Law
Experienced attorney and instructor with a demonstrated history of working in a multitude of legal areas. A strong legal professional skilled in intelligence law, cyber law, litigation, criminal law, and ethics. Over six years of experience both in and outside the courtroom, working with private and governmental entities.

Current Position
Army Judge Advocate General’s Corps, 2012 - Present
Captain in the United States Army serving under multiple commands and with numerous foreign partners. Advising Army Command Teams, prosecuting criminal cases, and instructing soldiers and civilian employees on legal matters. Working on multi-million dollar federal contracts and advising Commanders on the ethical appropriation and use of Government funds.

Notable Achievements and Contributions:
- Served in Afghanistan, Australia, Japan, South Korea, and the United States with a focus in national security law, cyber law, intelligence law, and military justice.
- Planned and executed a teaching program at the Army Intelligence Center on military information support operations with a special emphasis on cyber and electronic warfare.
- Served as a military prosecutor and Special Assistant United States Attorney as my primary assignment for over two years and worked on high profile cases such as US v. Sergeant Bergdahl.

Earlier Positions
- Assistant District Attorney, Milwaukee County, 2012
- Intellectual Property Research Assistant, Marquette University Law School, 2011 - 2012
- Intern, Wisconsin National Guard Staff Judge Advocate Office, 2011
- Lecturer of English Studies, Rangsit University, 2008 - 2009

Education and Credentials
- Judge Advocate Officer Basic Course - The Judge Advocate General’s Legal Center and School, 2013
- Juris Doctorate - Marquette University Law School, 2012
- Bachelor of Arts in Political Science - Northern Illinois University, 2008
- Bar Admission - Wisconsin State, 2012

Skills and Other Notes
- Fluent in both spoken and written Thai.
- Strong public speaking skills with an ability to communicate messages and lessons.
- Top Secret Security Clearance.
Experience

Commanded national-level offensive and defensive cyberspace operations teams.
- Fully trained in several distinct work roles within the Cyber Mission Force to include Team Leader, Exploitation Analyst, Network Warfare Cyber Planner, and Mission Commander
- Dual-appointed as a National Mission Team Leader within the Cyber National Mission Force for 12 months

Education

2017–Present PhD, Computer Science, University of Maryland, College Park, MD.
All but dissertation. Conducting digital security research with an emphasis on how people identify, assess, and respond to new digital security threats and vulnerabilities.

2017–Present MA, Nat’l Sec. and Strategic Studies, U.S. Naval War College, Newport, RI.

2015–2016 MS, Computer Science, University of Maryland, College Park, MD.
Graduated with a 4.0 GPA, inducted into Phi Kappa Phi Honor Society.

Inducted into Upsilon Pi Epsilon and Phi Kappa Phi Honor Societies.

Honors & Awards

Selected as one of four military fellows. Group focused on building a national strategy in the context of an increasingly digitized world.

2014 1st Place, Cyber Captain’s Cup, U.S. Cyber Command, Fort Meade, MD.
Served as the Team Co-Captain for the 2014 Army Cyber Knights. Won first place in the NSA/CSS/USCC Armed Forces Week Cyber Captain’s Cup competition out of 11 teams and nearly 200 Joint competitors.

2014 1st Place, 2014 Cyber 9/12 Student Challenge, Atlantic Council, Wash. DC.
The Cyber 9/12 Challenge was designed to offer students a better understanding of the policy challenges associated with cyber conflict. Our team achieved 1st place among 22 competing teams to include groups from Harvard, MIT, JHU, Carnegie Mellon, and Brown.

2013 Bronze Order of Mercury, Signal Corps Regimental Association, Fort Hood, TX.
The Bronze Order of Mercury recognizes those people who have demonstrated the highest standards of integrity, moral character, professional competence and selflessness.
Presentations

2017 Calcifying Cyber Readiness, USENIX LISA, San Francisco, CA.
2016 The New White Hat Hacking: Computational Biology for the Good of Mankind, DEF CON 24, Las Vegas, NV.
2016 Cross-platform Compatibility: Bringing InfoSec Skills into the World of Comp Biology, BSidesLV 2016, Las Vegas, NV.
2015 When CTFs Attack! Building a Better Training Environment, BSides Charm City 2015, Columbia, MD.
2012 Military Targeting Adapted for Hacking, Hacker Halted 2012, Miami, FL.

Publications

2017 User Interactions and Permission Use on Android, ACM SIGCHI 2017, Co-author.
2016 Summoning Demons: The Pursuit of Exploitable Bugs in Machine Learning, 2016 Reliable ML in the Wild, Primary author.
2012 Physical Security Threat from Hotel Wi-Fi, 2600 Magazine, Primary author.

Certifications

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Reverse Malware Engineer (GREM), GIAC Secure Software Programmer-Java (GSSP-JAVA), GIAC Penetration Tester (GPEN), GIAC Certified Network Analyst (GCNA), GIAC Certified Forensic Analyst (GCFA), Scrum Fundamentals Certified, PMP Project Management Professional, LPT Licensed Penetration Tester*, CEH Certified Ethical Hacker*, Security+, Network+, Certified Novell Administrator*

*Earned but did not pay for certification renewal
Experienced Cyber Threat Intelligence Researcher & Malware Analyst

Telework preferred
luiguibiker@gmail.com
linkedin.com/in/0x6c756973

(786)-298-4332
14383 136th Ct
Miami, Florida

Education & Certifications

Education
University of Central Florida, 2015, Orlando
M.S., Digital Forensics

Florida International University, 2009, Miami
B.S., Information Technology
with a minor in Criminal Justice

Miami Dade College, 2006, Miami
A.S., Computer Information Systems

Key Certifications
Expert
OSCP, Offensive Security Certified Professional
OSCE, Offensive Security Certified Expert
CCNA, Cisco certified Network Associate
COMPTIA A+ certified Computer Technician
COMPTIA NETWORK+ certified Network Technician
ALSO: GPEN, CEH, GCIH.

Telework preferred
luiguibiker@gmail.com
linkedin.com/in/0x6c756973

(786)-298-4332
14383 136th Ct
Miami, Florida

Specialized Skills

Public Work Samples

GitHub (GITHUB.COM/PUN1SH3R)
• Facebot: Facebook reconnaissance tools
• Indicators of Compromise (IOC) extraction tools
• Domain, malware, and miscellaneous testing scripts
• Public exploit discoveries found in DVD players and web servers available online
  (https://www.exploit-db.com/author/?a=6050)

Presentations
• HITRUST Feb 2016 briefing (http://www.aha.org/content/16/16febhitrusthhsbriefing.pdf)
• HITRUST March 2016 briefing
• Hackmiami conference 2014 (Facebot/https://sec-cons.net/talk/35933)
• CISCP Advanced Threat Technical Exchange (ATTE) June event (Evolution of Ransomware An Overview)
• Anomali detect conference 2016 (DGA Detection. Finding hidden malware without malware dissection)
BLOGPOSTS

- 3 Month frameworkPOS campaign nabs ~ 43 cc’s from POS systems (https://blog.anomali.com/three-month-frameworkpos-malware-campaign-nabs-43000-credits-cards-from-poi)
- NJrat Trojan case study (https://blog.anomali.com/njrat-trojan-alive-and-kicking-a-cool-overview-into-its-day-to-day-operati)

Programming & Scripting Proficiencies

- Proficient with Python, PHP, Perl, BASH, and familiar with most common Linux/Unix-shells (Bash,sh).
- Developed a tool to parse IOCs from several sources including but not limited to: PDF documents, text files, and web pages using Python. Available on Github.
- Developed a Facebook reconnaissance system as proof of concept (see Github).
- Expert proficiency with protocol analyzer tools; e.g. tcpdump, tshark and wireshark.
- Discovered two RCE zero day exploits on DVD player applications and Windows servers.

Professional Experience

UNIVERSITY OF ARIZONA SOUTH, (AZ) 10-17-PRESENT

ADJUNCT INSTRUCTOR

- Currently teaching CYBV/INFV 454 (Malware Threats and Analysis)
- Improve lectures, labs and overall structure of the course
- Help students to find a way into malware analysis by providing hands on and comprehensive insights from my experience in the field.

ANOMALI FORMERLY THREATSTREAM, REMOTE (MIAMI) 12-15-PRESENT

PRINCIPAL THREAT RESEARCHER (LABS R&D DIVISION)

- Developed an OSINT (Opensource intelligence) Bot in python order to improve IOC collection capabilities.
- Performed tracking and analysis of POS malware campaigns including but not limited to: Actors, infrastructure and instrumentation.
- Performed Threat actor tracking in darkweb markets (TheRealdeal, Alphabay, Rescator, Lampeduza, Exploit dot in).
- Developed configuration dumpers and network decoders for a variety of malware families.
• Performed memory forensics using Volatility framework.
• Performed Static malware analysis using IDA pro, hexrays decompiler and IDApython
• Wrote Intelligence and analysis reports for the following malware families: ProPOS, NJrat, Cryptohasyou, Cerber, FrameworkPOS, Spark POS, Katrina POS, Suppobox, Bartalex, XtremeRAT, Keybase, .
• Wrote intelligence reports on the following high profile leaks: Linkedin, Badoo, Twitter and Myspace.
• Developed Yara signatures in order to identify variants of new malware families.
• Configured and improved sandbox capabilities in the Threatstream TIP platform.
• Analyzed Macro based malware and tracked campaigns associated with them.

VERIZON CYBER INTELLIGENCE CENTER, REMOTE (MIAMI) 04/14-12-15

SR. CYBER THREAT INTELLIGENCE & MALWARE ANALYST

• Built a Malware analysis environment with opensource sandbox Cuckoo using an esx server with 20 analysis VM’s in order to perform dynamic and analysis on malware samples.
• Analyzed malicious office documents using oletools and Office malscanner. In order to extract valuable intelligence to be added into our threat database.
• Analyzed malicious pdf documents using jsunpack and spidermonkey. In order deobfuscate malicious content and extract valuable intel.
• Developed yara rules after malware analysis in order to detect and categorize malware families.
• Performed threat actor tracking using Maltego. as well as ThreatConnect.
• Developed a VirusTotal Dossier using virus total intelligence API in order to look for malicious metadata acquired from incident response engagements.
• Performed triage on suspicions PE binaries using the following tools: resourceHacker, peid and PE-view. In order to look for malicious artifacts that might lead to the identification of malware families.
• Performed tracking and research on the following crimeware malware families: dridex, neverquest/vawtrak, zeus, plugx, and the several POS malware families such as frameworkPOS, lucyPOS and backoffPOS.
• Performed tracking and research on the following ramsonware families: cryptolocker and torrentlocker.
• Analyzed windows forensic images using winhex and ftk imager. In order to extract valuable metadata that can enrich IR engagements.
• Performed windows registry forensics using registry viewer, regripper and yaru in order to hunt for artifacts that might lead to presence of malicious activity on the target system.
• Performed Malware analysis on samples acquired during IR investigations using tools such as: IDA pro, ollydbg, immunity debugger, tcpview, procmon, process explorer, and
tcpdump. the result of the analyses were added to the final deliverable that was handed to the customer.
• Performed dynamic binary analysis on ELF binaries using gdb, and strace, objdump and strings.
• Performed digital forensic analysis on disk images using, mmls,icat,fdisk,dd,fls,fsstat and blkcat as well as in-house developed tools.
• Performed memory analysis using volatility framework. On memory samples acquired from IR engagements.
• Developed automated feeds in python from threat data acquired via opensource intelligence in order to enrich our threat database.
• Developed a tool in python to parse IOC’s from email accounts related with crimeware groups. This effort helped gather more valuable intelligence to be stored on Verizon threat database.
• Developed a tool python to parse RSS feed in order to scrap ioc’s off blog posts including pdf documents.
• Responsible for multiple Debian-based Linux servers now instrumental to Verizon’s threat data cluster across the Verizon Communications enterprise.

Verizon Terremark, Secure Information Services, Miami, FL 04/12-04/14

Tier 3 Investigations Analyst

• Provided one to one mentorship to tier 1 analyst in information security related subjects in order to help them become more proficient in the subject.
• Developed a peer review system in php/jquery/mysql that allowed T2 analyst to grade Tier 1 performance.
• Developed a program that was initially developed in perl but then ported to python that would fetch packets using netwitness api in order to allow the analyst to be able to perform analysis faster.
• Developed a tool made in bash that fetched malicious ip addresses from sites that contained ip reputation data in order to feed it into NW api in order to look for adversary activity.
• Developed a snort ID lookup tool in php/mysql in order to facilitate the search of snort rules.
• Performed network forensics using the following tools: tcpdump,tshark and Wireshark.
• Perform network traffic analysis in order to look for adversary activity using nfdump, and netwitness.

Securabit Group, Richmond, VA 06/12-PRESENT

Lab Doctor/Bot creator
• Support and maintain securabit infrastructure that comprises of a cluster of esx 5.1 hosts
• Support and maintain a community based penetration testing lab where folks can freely go and learn hacking techniques without getting in trouble.
• Developed a series of bots written in python in order to automate virtual machine administration on the Penlab. This helped reduce admin
• Configured Zabbix in order to monitor the securabit infrastructure.
• Develop a bot in order to automate the registration system for the penlab using python.
• Developed challenges for CTF engagements in the area of penetration testing.

11TH JUDICIAL CIRCUIT COURTS, MIAMI, FL

NETWORK MANAGER

• Monitored network traffic using NFDUMP and firewall analyzer in order to detect abnormal traffic patterns related with computer intrusions.
• Performed in-house white-box penetration testing using metasploit framework as well as core impact and Nessus. The goal was to identify vulnerable hosts in order to minimize the chance of a computer intrusion.
• Performed binary static/dynamic file analysis of malware samples acquired from compromised systems, using immunity debugger, windbg, ollydbg , tcpview and process monitor. The results of this analysis allowed the court to create better IDS signatures in order to foil intrusions.
• Maintained/managed Cisco based Wireless infrastructure of Cisco 1240 AP’s, using Cisco ACS. This project allowed case managers and court personnel connect wirelessly to the court network while in court session.
• Maintained/installed Trend-micro officescan 10 Anti-virus Cluster . The maintenance of these servers allowed court desktops to have the latest antivirus definitions that prevented many intrusions related with malware.
• Developed scripts to automate router/switch/AP management using python. These scripts allowed faster management of network gear cutting support time almost 50%.
• Developed scripts to automate user creation, mailbox management, group allocation using vbscript and powershell. These scripts allowed streamlining the creation/configuration of email boxes for users when the court had a hiring spree of 200 employees.
• Maintained and managed Bluecoat sg 600 web proxy appliance. The configuration of this appliance allowed the court to reduce web related attacks and infections by 70%
• Maintained and performed patch management using Ms Wsus and sscm server.
• Performed port scanning and network reconnaissance using nmap
• Performed web-app vul scanning and analysis using w3af, wfuzz, burp proxy against the court public facing website.
• Maintained/monitored Ironport C160 mail proxy cluster. In addition, I also created content filters and monthly reports to be able to track and stop spam/malware.
• Maintained Cisco infrastructure that consisted of cisco 6509 and cisco 3750 multilayer switches. Having these devices maintained in house allowed us to save almost 90% of support cost.
• Monitored Juniper IDP 250 ids appliance for unusual network activity and network attacks.
• Created custom attack signatures to foil network attacks on juniper idp 250 based on data gathered on honeypots and log data from splunk servers.
• Maintained Vmware vsphere virtual environment along with it back-end Storage SAN Xiotech emprise 5000 appliance
• Performed incident handling when network threats were present.
• Maintained and configured Splunk server for log parsing and analysis of firewall and IDS data in order to hunt for intrusions.

• Bilingual in English and Spanish
• References available upon request
Troy J. Ward
134 Idlewilde Rd. ● Severna Park, MD ● 21146
254-423-1181 ● Troy.J.Ward80@gmail.com

Top Secret/SCI With CI Polygraph

Professional summary
Accomplished network security professional with the proven ability to lead teams. Extensive experience conducting defensive cyber operations (DCO) on strategic and tactical networks looking for malicious activity. Innovative out of the box thinker who can analyze networks using both indicators of compromise (IOC) as well as traffic profiling and anomaly detection techniques. Serves as the technical director for multiple Title-10 offensive cyber networks. Key skills include:

- Personnel Management
- Network Analysis
- Cyber Security
- Intrusion Detection Systems
- Python
- Splunk Power User

Experience

Defensive Operations
- Conducted multiple DCO and incident response missions on Department of Defense (DOD) network utilizing new and advanced analytical techniques to find previously undiscovered adversary traffic; Created practical implementations of latest academic research.
- Used intelligence from both within the Intelligence Community (IC) as well as external sources to profile potential adversaries and develop passive techniques to identify their presence on networks.
- Developed SNORT signatures as well as Bro scripts to identify IOCs gleaned through Signals Intelligence (SIGINT) and packet analysis with Wireshark and other tools.
- Taught advanced adversary hunt techniques to approximately 100 other DOD defenders.
- Developed advanced Splunk dashboards which used statistical methods to visualize and identify anomalies in network traffic through the examination of various sensor logs. Focused on user behavior profiling to identify credential abuse and user impersonation.
- Used active and passive tools to enumerate networks and identify potential vulnerabilities.
- Officer in Charge and flag developer for the 5th annual Army Cyber Skills Capture the Flag competition.

Offensive Operations
- Serves as technical director for multiple Title 10 offensive cyber platforms; act as subject matter expert on mission design and infrastructure operation.

Network Operations
Engineered and maintained tactical networks of various classifications supporting 5000+ users across geographically dispersed areas.
Configured and secured tactical networks with firewalls and access control lists (ACL).

Communication
Coordinated sharing of information and intelligence through various departments and agencies increasing the overall efficiency of adversary hunt operations.
Coached and mentored 500+ Soldiers on advance techniques related to tactical communications while they trained at the National Training Center.
Developed curriculum for advanced network operator course at the US Army Signal Center of Excellence; training received by 200+ people per year.

Supervision
Supervised a mission team consisting of approximately 20 people from multiple agencies tasked with identifying adversary presence on various networks.
Led a team of 20 satellite controllers responsible for the day to day operation of three DOD satellites worth in excess of $2B with zero loss of services.
Senior watch officer for the Cyber National Mission Force coordinating the daily activity of approximately 1,500 cyber operators.

Employment History
- Offensive Operations Technical Director ● United States Army ● 2018 – Present
- Defensive Cyber Mission Lead ● United States Army ● 2015 – 2018
- Communications/Network Security Trainer/Mentor ● 2012 – 2015
- Satellite Operations Officer ● 2010 – 2012
- Network Engineer ● 2007 – 2010

Education and Certifications
- Masters of Science in Information Assurance ● Norwich University Northfield, VT ● 2015
- Bachelors of Arts in Information Systems Management ● University of Maryland University College Adelphi, MD ● 2013
- Intermediate Cyber Course ● National Cryptologic School ● 2015
- Network Engineer Officer Training Course ● United States Army ● 2012
- Network Operations Advanced Training Course ● United States Army ● 2000
- COMPTIA Advanced Security Practitioner Certification ● 2018
- GIAC Network Forensic Analyst Certification ● 2016
- GIAC Continuous Network Monitoring Certification ● 2016
- Cisco Certified Network Associated ● 2015
• Splunk Power-User Certification • 2017

Publication and Presentations

• Owner and primary writer of www.signal-chief.com
• Developer of the Facebook Capture the Flag Splunk app
• Github located at https://github.com/pyrodie18
• Presenter at 1st quarter 2018 NSA Splunk Conference “Identification of Golden Tickets and other advanced APT analytics with Splunk”
TURE PEKEN
(+1) 520-891-8360 • turepeken@email.arizona.edu • 2115 E 2nd St 85719 • Tucson, AZ

EDUCATION

University of Arizona, Tucson, AZ
PhD in Electrical and Computer Engineering (GPA:3.83/4.00)

University of Michigan, Ann Arbor, MI
Master of Science in Electrical Engineering: Systems with major on Communications (GPA:3.34/4.00)
- Coursework: Digital Communication and Coding, Communication Networks, Stochastic Processes,
- Probability, Mathematical Methods for Signal Processing, Game Theory, Real Time Computing

Istanbul Technical University, Istanbul, Turkey
Dual Bachelor of Science in Telecommunications Engineering and Computer Engineering (GPA:3.69/4.00)
- Ranked 3rd in Telecommunications Engineering and 4th in Computer Engineering

SKILLS


WORK EXPERIENCE

Keysight Technologies, Santa Rosa, CA
Intern R&D Engineer
- Worked on 5G New Radio Technologies
- Physical channels and channel encoder were implemented based on TS 38.211 and TS 38.212 using MATLAB
- A novel hybrid beamforming algorithm for 5G was developed and integrated into SystemVue

Keysight Technologies, Santa Rosa, CA
Intern R&D Engineer
- Worked on channel estimation for massive MIMO
- Implemented pilot-based, semi-blind, and blind channel estimation algorithms by using C
- Integrated channel estimation algorithms with SystemVue

Netas, Istanbul, Turkey
Software Design Engineer
- Worked on software design of LTE-Advanced eNodeB for uplink
- Focused on LTE physical layer design and developed channel estimation and equalization algorithms for the receiver of the eNodeB
- Implemented the algorithms by using C in Code Composer Studio
- Tested the algorithms on TCI6638K2K

Isnet A.S., Istanbul, Turkey
Satellite System Engineer
- Monitored, configured, managed and maintained network devices of Cisco, Hughes and Gilat to provide reliable data and voice services to customers through satellite network

RESEARCH EXPERIENCE
University of Arizona
Research Assistant with Prof. Tamal Bose
Sept. 2014-Present
- Research on spectrum sharing between MIMO radar and MIMO communication system
  o Published a paper in WinnComm 2015
- Research on blind channel estimation for massive MIMO
  o Published a poster in BWAC 2015 and a paper in WinnComm 2016
- Research on channel estimation with compressive sensing methods for massive MIMO
  o Published a poster in BWAC 2016 and a paper in ITC 2017
- Research on hybrid beamforming for massive MIMO in millimeter-waves
  o Published a paper in WinnComm 2017

University of Michigan
Independent Research
- Research on LDPC codes and Belief Propagation Decoding Algorithm
- Analyzed the performance of decoding LDPC codes with Belief Propagation Decoding Algorithm via MATLAB
- Research on Bayesian Learning in Social Networks

TEACHING EXPERIENCE
University of Arizona
Teaching Assistant
Jan. 2017-May 2017
- Worked as a consultant for Ephibian
- Provided the necessary information to Ephibian for developing CellSim, which is a simulator for cellular networks (CDMA, UMTS, LTE).

University of Arizona
Teaching Assistant
Jan. 2017-May 2017
- Instructor of Wireless Networks and Security (CYBV 479)
- Taught wireless technologies, mobile protocols, mobile identifiers, mobile and location-based services, mobile encryption standards.

University of Arizona
Teaching Assistant with Garrett Vanhoy
Sept. 2015-May 2016
- TA for Microprocessor Organization (ECE 372A)

University of Arizona
Teaching Assistant with Prof. Wolfgang Fink
- TA for Computational Techniques (ECE 330)

University of Arizona
Teaching Assistant with Prof. Ali Bilgin
Sept. 2014-Dec 2014
- TA for Applications of Engineering Mathematics (ECE 310)

PUBLICATIONS
Experience

Intelligence Specialist
Defense Strategic Debriefing Course, Fort Huachuca, AZ

November 2014 – Present

Provide platform instruction for groups of up to 64 students to support the DSDC mission of certifying strategic debriefers for the Defense HUMINT Executors. Roleplay 13 different sources from diverse backgrounds during one-on-one collection events to provide students with a challenging and realistic interaction to enhance their learning. Develop, maintain, and update my 13 assigned roles in support of the Defense Strategic Debriefing Course’s (DSDC) full continuum of operational strategic debriefing environments. This role development includes conducting research into contemporary international issues and technical areas to include cybersecurity issues. Provide subject matter expertise into the development of cyber roles to ensure realism. Provide students with an in-depth and timely critique of their performance during training events to identify and improve both shortcomings and strengths. Provide retraining to students who have failed to meet the performance standards either during collection events or intelligence reporting to ensure stronger performance during the subsequent training event.

Instructor

Joint Senior Interrogator Course, Fort Huachuca, AZ

August 2011 – November 2014

Conducted platform instruction, using the Small Group Instruction Technique, for classes of up to 16 students. Imparted knowledge regarding the best practices in mentoring and supervising junior interrogators. Provided supervision and mentorship to Joint Senior interrogator Course (JSIC) students during their interaction with Human Intelligence Collector Basic Course (HBCBC) students during the HBCB capstone exercise. Evaluated, edited, rewrote, and developed instruction plans in order to maintain currency with current Army doctrine and law enforcement techniques. Acted as a role-player, accurately portraying detainees from various Areas of Operation. In the absence of the JSIC director, I updated and prepared the JSIC Critical Task Cross-walk, to include lesson plans, practical exercises, and evaluations standards for presentation to the Training Review Board, which consisted of representatives from each of the Defense HUMINT Executors. Represented JSIC as a member of HT-JCoE’s curriculum mapping committee, ensuring the accurate integration of the material taught at JSIC into HT-JCoE’s university learning model. Conducted platform instruction, using the Small Group Instruction Technique, for classes of up to 16 students. Imparted knowledge regarding the best practices in mentoring and supervising junior interrogators.
Provided supervision and mentorship to JSIC students during their interaction with Human Intelligence Collector Basic Course (HBCBC) students during the HBCB capstone exercise. Evaluated, edited, rewrote, and developed instruction plans in order to maintain currency with current Army doctrine and law enforcement techniques. Served as an observer/controller evaluating interrogator performance in support of pre-deployment certification training for three separate Military Intelligence battalions at the INSCOM Detention Training Facility.

**Instructor**

Joint analyst Interrogator Collaboration Course, Fort Huachuca, AZ

*March 2010 – August 2011*

Provided platform instruction to classes of up to 52 students. Created and updated lesson plans. Served as small group leader to guide and mentor students. Performed duties as a role-player, accurately portraying detainees from the class’ target Area of Operations. Thoroughly evaluated, graded, and reviewed student performance during training exercises. Provided retraining to student whose performance did not meet the course standards, to remediate their weaknesses and help them achieve the required level of competency in their job skills.

**Company First Sergeant**

United States Army, Fort Hood, TX

*November 2007 – February 2010*

Enforced military standards and physical fitness while supervising the individual training and care of 64 Soldiers in 4 military occupational specialties. Provided guidance and administrative support for 1 Operational Management Team (OMT) and 10 HUMINT Collection Teams (HCT) during one deployment in support of Operation Iraqi Freedom. Supervised the maintenance and accountability of 15 intelligence systems, 4 vehicles and other unit equipment valued in excess of $2 million. Advised the commander on matters pertaining to enlisted personnel, regulations, and operational matters. Ensured that all paperwork met the standards for proper format, grammar, and accuracy. Produced and reviewed reports for dissemination at all levels, and conducted briefings to both higher and lower echelons.

**Debriefer**

Defense Intelligence Agency, Stuttgart, Germany

*August 2004 – November 2007*

Planned, developed, and implemented collection strategies in support of national and theater-level consumers. Identified and located sources of national-level interest, assessed their knowledge and capability, and conducted debriefings. Prepared and transmitted notices of intelligence potential, wrote and disseminated collection reports to national and theater-level consumers in response to standing requirements, operating directives, and ad hoc taskings. Deployed and conducted Military Source Operations in support of Operation Iraqi Freedom. Deployed to Bosnia in support of the NATO mission to capture persons indicted for war crimes.
Senior Interrogator
United States Army, Fort Bragg, NC

June 2001– August 2004

Served as a HUMINT section team leader and senior interrogator/strategic debriefer for a Military Intelligence Detachment supporting a 1,300 soldier Special Forces group. Managed all aspects of counterintelligence and interrogator soldier skills and mandatory training for a four soldier team. Maintained accountability for the operation, maintenance, and security of all team equipment, valued at over $300,000. Served as Operational Control Element Noncommissioned Officer in Charge, conducted debriefings of Special Reconnaissance teams, and conducted force protection during my first deployment in support of Operation Enduring Freedom. Conducted Military Source Operations, Key Leader Engagements, and interrogations during the second deployment in support of Operation Enduring Freedom. Provided expert role-player support on two separate occasions to the Advanced Special Operations Techniques Course taught by the John F. Kennedy Special Warfare Center and School.

Military Language Instructor
United States Army, Monterey, CA

January 2000 – June 2001

Served as a Military Language Instructor at the Defense Language Institute, Foreign Language Center. Conducted classroom, laboratory, and special foreign language instruction, and taught vocabulary, grammar, and military related skills to 30 joint service students during an extremely demanding 63 week course. Prepared class materials, evaluated student strengths and weaknesses and advised commanders on student potential for retainability as military linguists. Counseled students on academic and disciplinary issues. Supported the U.S. Army Recruiting Command on two separate occasions by traveling to high schools and giving presentations on the Army’s linguist programs.

Training Platoon Sergeant
United States Army, Monterey, CA

April 1998 – January 2000

Led, evaluated, and trained a platoon of 50 Initial entry training soldiers studying Arabic and Hebrew at the Defense Language Institute, Foreign Language Center. Conducted physical fitness training, ensured personnel accountability, inspected barracks to ensure proper maintenance. Counseled soldiers on military, academic, and personal matters. Initiated and followed up on promotion, personnel, and finance actions. Ensured health and welfare of soldiers and their families, and resolved soldiers’ personal and military issues. Planned and oversaw the conduct of the land navigation lane during four iterations of the Language Training Exercise, providing students with a challenging and winnable test of both their language and land navigation abilities.

Interrogator Advisor
United States Army, Fort Bragg, NC
February 1994 – February 1996

Served as an interrogator for an airborne psychological operations group. Responsible for the health, welfare, and physical preparedness of six soldiers. Oversaw day-to-day operation of the group S-2 section, managing the group personnel security program to include editing, directing, and tracking the submission of all personnel security investigation packets within the group. Assisted in the management of the Special Operations Debriefing and Retrieval System (SODARS) program; directed all SODARS collection and reporting requirements within the group.

**Interrogator**

United States Army, Darmstadt, Germany

February 1990 – January 1994

Deployed as part of a military intelligence brigade supporting an army corps during Operations Desert Shield and Desert Storm. Utilized interpreters to conduct interrogations of enemy prisoners of war and deserters to obtain information necessary for the development of military intelligence. Provided translation and administrative support to the liaison office between the U.S. Army Fifth Corps and the German Fourth Defense District Command. Supported the U.S. Army’s Fifth Military Intelligence Company by performing German language document exploitation. Provided translation support to NATO’s annual Return of Forces to Germany exercise. Performed research into cultural and ethnic issues for the purpose of developing briefing packets for United States Army Europe personnel preparing to deploy in support of NATO operations during the Yugoslavia Civil War.

---

**Education and Training**

**Master’s of Science in Cyber Security**

University of Maryland University College, Adelphi, MD

December 2017

Maintained a 4.0 GPA through the entire course

**Bachelor’s of Science in Liberal Arts**

Excelsior College, Albany, NY

June 2007

Maintained a 4.0 GPA through the entire course

**Associate’s of Arts in Foreign Language**

Monterey Peninsula College, Monterey, CA

May 2001

Double major in German and Arabic; Graduated Cum Laude

**Small Group Instructor Training Course**

United States Army Intelligence Center of Excellence, Fort Huachuca, AZ

November 2011

**Instructor Training Course**
Defense Language Institute, Monterey, CA

May 2000

**Skills and Abilities**

Currently developing the curriculum for University of Arizona course CYBV435 (Cyber Threat Intelligence)

Currently hold a Top Secret level security clearance

Served as intelligence subject matter expert for Carnegie Mellon University’s cybersecurity exercises

Working proficiency in Python

Studied Cobol

Studied Basic

Excellent proficiency in the German language

Basic proficiency in the Arabic language

**Leadership**

I have served in multiple leadership positions during my military service, ranging from squad leader to first sergeant in an intelligence company during time of war. This experience has helped me as an instructor by providing me with multiple ways to communicate with students and assist them in the adult learning process. Additionally, as a civilian employee of the Department of Defense, I have temporarily filled leadership positions during my supervisor’s absence, and represented my course to other elements within my organization.

**References**

**Steven Frelke, HT-JCoE**

(520) 538-4300, steven.r.frelke.civ@mail.mil

**Patrick Skora, HT-JCoE**

(520) 533-7925, patrick.a.skora.civ@mail.mil

**Kelly Sanders, HT-JCoE**

(520) 538-9003, brookshear.sanders@us.army.mil
Jordan VanHoy

2689 S Gabriela Ave  
Yuma, Arizona  
(910) 585-3626  
jordanvanhoy@yahoo.com

PORTFOLIO TABLE OF CONTENTS

RESUME.............................................................................................................. 2
REFERENCES.......................................................................................................... 6
CERTIFICATIONS AND TRAINING................................................................. 7
TRANSCRIPTS........................................................................................................ 8
STATEMENT OF SERVICE................................................................................... 9
Jordan VanHoy

2689 S Gabriela Ave (910) 585-3626
Yuma, Arizona jordanvanhoy@yahoo.com

PROFILE

I am a highly motivated, detail oriented individual with solid leadership experience. I have a passion for educating and fostering creative thought in the minds of the upcoming cybersecurity generation.

EDUCATION

Masters of Science Cybersecurity Studies 9/2018 American Military University
Charles Town, WV Cumulative GPA: 3.94/4.0

Bachelor of Science Information Systems Security 11/2014 American Military University
Charles Town, WV Cumulative GPA: 3.01/4.0

Undergraduate Certificate in Digital Forensics 08/2016 American Military University
Charles Town, WV Cumulative GPA: 3.94/4.0

EXPERIENCE

Air Intelligence Officer 01/2015- Present
Marine Aircraft Group 13 Yuma, Arizona

- Principle advisor on all intelligence matters for 253 employees. On a daily basis, a high level of analytics are conducted in order to present briefings to the president of the organization. Direct training and oversight of nine employees in the intelligence department.
- Security and Risk Management through the compliance of intelligence oversight and executive order 12333.
- Multi-domain achievement in the common body of knowledge through the appointment of Physical Security Manager for the organization. Duties included designing, implementing, and enforcing visitor control, physical control barriers, and writing policy level documents governing the physical security of the building.
- Appointed the Communications Officer for the squadron providing for asset protection, configuration of software and cryptographic functions. Additional duties included software and hardware acquisition, leadership and direction for five system administrators, and developing user awareness training.
• Establish handling requirements for classified information inside of the intelligence department and compliance with classification guidelines.

Special Intelligence Communicator/System Administrator 04/2014-01/2015
1st Radio Battalion Camp Pendleton, California

• Supervisor for a department of 53 communication Marines. Daily duties included maintaining administrative requirements, scheduling training, and project management.

Digital Network Analyst 01/2013-04/2014
National Security Agency Fort Meade, Maryland

• Offensive survey analyst in the Network Analysis Center. Primary duties were to analyze metadata for relevant intelligence information and supply customers with material pertaining to targets of interest.
• Provided for Identity and Access management by implementing and enforcing multi-factor authentication to networks and office spaces.
• Security Assessment and Testing experience through the application of internal and third party audits to ensure integrity of searches and compliance with executive order 12333.

Special Intelligence Communicator/System Administrator 01/2012-01/2013
Deployable Communication Operations Fort Meade, Maryland

• Security engineering by developing network design, configuration, and implementation of Cisco routers, switches, and Cisco ASA 5510 firewalls onto sensitive networks spanning several classifications.
• Asset protection through frequent inventory and enforcement of physical defense in depth to sensitive assets. Assets were required to be locked in General Services Administration safes, and utilization of SF-700 series documentation.
• Identity and access management by managing physical access into sensitive areas by use of joint personnel adjudication system to verify security clearance data. This duty frequently required escorting individuals through controlled areas. Additionally, duties included ensuring physical security controls adequately prevent unauthorized individuals.
• Provided support in Telecommunication and Network Security while working with the Trojan LITE. The Trojan LITE enables expeditionary satellite communication and network connectivity across multiple classifications. Daily duties included configuring local area networks on Cisco switches and routers and establishing X-band satellite communication.

Special Intelligence Communicator/System Administrator 08/2010-01/2012
Marine Cryptologic Support Battalion Fort Meade, Maryland
• Network administrator within a five man team that managed 315 assets of varying classifications and 300 users. Daily duties included managing user public key infrastructure, user accounts, permissions, and the protection of classified information and assets.

• Other duties pertaining to Security and Risk Management and Security Operations included coordinating the yearly emergency action plan exercises for business continuity, and leading after action reporting.

• Experience in Communications and Network Security by configuring and maintaining computer software, websites, and databases supporting 300 users spanning multiple classification levels, ensuring system requirements align with business and user-specific needs. Provide leadership and direction for a team of 4 system administrators tasked with promoting optimal system performance, reliability, and uptime.

Special Intelligence Communicator/System Administrator 03/2009-08/2010

1st Special Security Communications Team Okinawa, Japan

• System administrator of 25 assets of varying classifications. Daily duties included asset and data protection through the use of physical and technical controls to ensure zero data spillage between networks, or accidental information disclosure.

• Telecommunication and network security while working with the Trojan LITE. The Trojan LITE enables expeditionary satellite communication and network connectivity. Daily duties included configuring local area networks on multi-model Cisco switches and routers and establishing X-band satellite communication.

• Security and Risk Management experience writing business continuity plans, emergency action plans, and disaster recovery plans. These plans typically covered the continuity of critical communication equipment and networks, and the destruction of classified documents and assets.

• Further daily duties included maintenance of cryptographic equipment to include KG-175D. Duties encompassed providing secure communications across the Okinawa, Japan region and the configuration of multi-model Cisco routers and switches.

Special Intelligence Communicator/System Administrator 07/2008-03/2009

Military Job training Pensacola, Florida

• Systems Administrator duties encompass all-inclusive encrypted communications with tactical radio platforms, satellite platforms, and data network services from local-level to enterprise-level designs which include but not limited to specialized communications equipment, unit-unique intelligence repositories and computer information technology, and the integration of enterprise services, automated services, cloud computing, converging and emerging technologies, and national-to-tactical reach back capabilities.

• This duty also maintains connectivity into the Marine Corps ISR enterprise for data standardization, enterprise support and services, network and data redundancy, and disaster...
recovery. Additionally, Marines assigned this MOS will receive training in computer hardware fundamentals, common operating systems, network security, information assurance, database and data flow management, radio frequency theory, satellite communications, basic, intermediate and advanced networking, network and data science philosophies, information warfare, and cyber security policies.

Jordan VanHoy
REFERENCES

Ricardo Moreira, Direct Supervisor, 2016-2018
Intelligence Officer, Marine Aircraft Group 13
Work Phone: 928-269-5669
Email: Ricardo.moreira@usmc.mil

Samuel Winsted, Direct Supervisor, 2016-2018
Intelligence Officer, Marine Aircraft Group 13
Work Phone: 928-269-2413
Email: Samuel.winsted2@usmc.mil

Eldar Krueger, Direct Supervisor, 2009-2012
Telecommunications and Network Security Chief, 1st Special Security Communications Team
Work Phone: 240-373-1682
Email: eldar.krueger@usmc.mil

Jordan VanHoy
CERTIFICATIONS AND TRAININGS

- CompTIA Network+ (Career ID: COMP001008910598)
- Cisco Certified Entry Level Network Technician (Cisco ID: CSCO12209538)
- CompTIA Security+ (Career ID: COMP001008910598)
- CompTIA CySA+ (Career ID: COMP001008910598)
- ISC² Certified Information Systems Security Professional (ID: 636945)
- Top Secret/Secret Compartmented Information active clearance
- Counterintelligence Polygraph
Kate (nee Hansen) Mabbett
953 West Golden Barrel Court ~ Oro Valley, Arizona 85755 ~ 202-905-8637 ~ khansen7@gmail.com

Customer-obsessed, proven leader in customer success management, cyber operations and cybersecurity across both industry and government.

Summary

- Active Top Secret/SCI
- International Experience
- Certified Ethical Hacker, August 2016
- Member of Women in International Security (WIIS), Washington, D.C. Chapter January 2014 - Present

Professional Experience

IronNet Cybersecurity
Vice President Customer Success
April 2017-Present
March 2018-Present
- Actively managed $26.5M of revenue from current customers while growing base with future expansion into operating companies affiliated with current customers. Advanced right-sizing (upsell) for key customer driving all planned sales for 2019-2021 into 2018 calendar year. A leader within IronNet, developed first-ever procurement process guide detailing customer care and company processes ensuring accurate ordering, tracking and invoicing. Crafted the IronNet communications guide, a company-wide policy for improving communications both externally with customers and internal to the company.

Customer Success Manager
April 2017-March 2018
- Responsible for managing the entirety of a customer relationship starting at contract signature through the life of the partnership. Served as the primary point of contact for customers across both large energy utilities companies as well as the financial sector.

Office of the Director of National Intelligence
Cyber Intelligence Officer, Cyber Threat Intelligence Integration Center
November 2015-April 2017
- CTIIC founding member, provided timely analysis and threat reporting to senior US Government officials. Regularly informed the Presidential Daily Brief and National Security Council sessions with analysis and strategies to counter foreign cyber threats to U.S. national interests.

Department of Defense
Strategic Mission Review and Innovation Team, Agency Director Staff
September 2008–November 2015
- Handpicked to serve on Agency Director’s staff, provided recommendations to senior leadership for improving current missions, functions, capabilities ensuring continued innovation.

Chief Operating Officer, NETCRAFT
November 2014 – November 2015
- Led a small team to develop, evaluate and transition key technologies for improving cybersecurity of unclassified Internet activities creating efficiencies in intelligence analysis. Worked closely with industry partners to test new technologies on DoD architecture for faster acquisition and integration. Transformed operational authorities for improved analysis while ensuring civil liberties and privacy are protected.

Branch Chief, Middle East and Africa
August 2013 - November 2014
- Created the Middle East and Africa Cyber Team to investigate, develop and deploy cyber countermeasures through the area of operations. Informed the President’s Daily Brief during several high-priority international events. Delivered game-changing analysis shifting U.S. defense priorities.
Branch Chief, Discovery Technology Exploitation November 2011 - August 2013

- Executed mission and resource alignment review resulting in reallocation of 40% of resources, re-oriented investment structure for both innovation and personnel to ensure strategic alignment with senior leadership objectives. Created efficiencies by revolutionizing the tasking process for key accesses freeing up 20% of resources for new capability testing and evaluation.

Special U.S. Liaison Office London Support to High Priority Event August 2012 - September 2012

- Crafted real-time reporting across both U.S. and U.K. Government agencies providing critical analysis to the White House, Downing Street and U.S. Ambassador to the U.K. Ensured decision makers across both Governments were postured to best protect and defend against potential security threats throughout the event. Developed and implemented business plan for sharing unprecedented capabilities between the U.S. and U.K. Governments to quickly identify, investigate and mitigate or thwart potential attack vectors.

Executive Assistant to the Special U.S. Liaison Officer London June 2010 - November 2011

- Conducted comprehensive evaluation of current and future U.S. and U.K. cyber technology investments, specifically assessing degree of alignment in overall priorities. Focused on potential cost-sharing initiatives and complementary projects for future capabilities to improve alignment and reduce redundancy.

Assistant Crisis Event Lead Counterterrorism Mission Management Center May 2010 - June 2010

- Drove to closure multiple high-impact efforts while leading a cross-organizational team of diverse talents and skills to meet increasing demands for support. Team consisted of partners from across the U.S. and ally Governments. Crafted daily updates for U.S. Government senior leadership informing the White House of current efforts, successes and gaps.

Intelligence Analysis Development Program September 2008-May 2010

- Developed skills and competencies as an analyst with tours of service across the Department of Defense.

Education

University of Maryland University College; Master of Science Cybersecurity; Conferred May 2016

Department of Defense Intelligence Analysis Development Program; Specialized in digital network analysis, geospatial metadata analysis and crisis event support; Conferred May 2011

University of Kentucky; Bachelor of Arts Arabic and Islamic Studies; Bachelor of Arts International Relations; Conferred May 2008

University of Iowa; Bachelor of Arts French Language and Culture; Conferred August 2006

National Cryptologic School; Various courses related to Signals Intelligence (Reporting, Traffic Analysis, SIGINT Development, Digital Network and Geospatial Analysis), Information Technology, Telecommunications, Organizational Design and Leadership; September 2008 - Present

Significant Awards, Promotions

- Promoted to Vice President Customer Success in less than one year with IronNet.
- Letters of appreciation from Director NSA/Cyber Command, Deputy Director NSA, Deputy Director for Data Acquisition, Commanding General of U.S. Army Cyber Command.
- In Department of Defense earned 4 promotions in 5 years, annual agency promotion rate is the top 3%.
Henry A. Werchan

715 E. University Blvd. (520) 205-1560
Tucson, AZ 85719 henry.werchan@gmail.com

OVERVIEW

Thirty years hands-on, technical, management and leadership experience in developing and deploying complex network management and security systems. Proven record in adapting and deploying commercial off-the-shelf products in support of complex system requirements. Well versed in scrum agile based systems and software engineering and development as well as project management.

PROFESSIONAL HISTORY

Principal Engineer & Program Manager General Dynamics 2005 - Present

Responsible for network and security management across General Dynamic programs. Includes definition and refinement of operational concepts and derived requirements, design review and feedback, identification and pursuit of business opportunities, and liaison and interaction with the government, user community, and other companies and organizations.

• Interface with customers and user communities to determine requirements and translate these into operational needs and system deployments and upgrades.

• Define technical solutions in support of current and emerging programs; identify applicable hardware and software solutions.

• Provide input and guidance to internal research and development programs to ensure investment is aligned with customer trends and capabilities.

• Implementation of unified information security solutions based on the NIST Risk Management Framework.

• Scrum agile based development of cloud computing security management system.

• Penetration testing and security vulnerability assessment and analysis.

Senior Member of the Technical Staff The MITRE Corporation 1999 - 2005

Technical lead for communications, network and systems management, and information security for government and military organizations worldwide.

• Designed and implemented network and security management capabilities, including development and fielding of an appliance-based device to monitor bandwidth utilization, protocol distribution and intrusion detection.

• Designed and implemented a fiber based local area network for tactical command posts as part of a converged network design including streaming video, voice over IP and other network-based services. Decreased deployable cable infrastructure by 90%.
**Business Area Technical Lead**  Ephibian Incorporated  1996 - 1999

Technical lead for a startup company in the network and security management business area. Provided systems engineering and operations support to major commercial and government customers. Business model culminated in a multimillion dollar evaluation within three years, with a corresponding employee growth from seven to 30+.

- Led technical and business development effort in building a world class network operations center in support of a major airport internet kiosk provider and other commercial customers.

- Established network operations center for the State of Tennessee Department of Education K-12 education network.

**Communications Officer**  The United States Army Reserve  1991 - 1995

Communications officer for an armor battalion. Executed the first deployment of frequency hopping radio technology within the U.S. Army Reserves.

**Member of the Technical Staff**  The MITRE Corporation  1991 - 1996

Technical and project management lead for systems engineering activities in the areas of network and systems management, distributed and client-server systems, information technology, and communications. Hands on experience with rapid prototyping and integration of commercial off-the-shelf products.

**Communications Officer**  The United States Army

Responsible for communications engineering, automation, and network and security management. Planned, engineered, and managed voice and data communications networks deployed world-wide. Engineered and managed the Army’s deployed communications network during operation Desert Storm.

**Education**

Enterprise Security Certification, The University of Arizona  2015

Master of Science Electrical Engineering, The University of Arizona  1992

Bachelor of Science Electrical Engineering, Texas A&M University  1986

**Certifications**

SAFe 4 Certified Scrum Master

CNSS 4011: Information Systems Security Professional

CNSS 4012: Senior Systems Manager

CNSS 4013: Systems Administration

CNSS 4016: Risk Analyst
LINDA L. DENNO, Ph.D.

3678 Plaza de la Rosa
Sierra Vista, Arizona 85650
(520) 803-8169
Email: ldenno@epic-cas.org

QUALIFICATIONS
As an educator and political scientist, I have many years of experience in the fields of education, politics, and administration. I have taught, researched and wrote about all aspects of politics, including public policy and law, cyber law and policy, elections and the electoral process, and government systems. I have served on and chaired numerous committees, including policy committees and committees of an administrative nature. I have supervised research assistants, graduate students, clerical and professional staff and junior faculty and teachers. I have taught undergraduate and graduate students at the university level. I have advised political actors and have been recognized as an expert political analyst, speaking and writing for news media and appearing on television and radio. I have written successful grant proposals, planned and coordinated conferences and administered state and federal programs.

EDUCATION
1986-1991 Ph.D. Political Science, University of California, Davis
    Dissertation: The Nomination and Confirmation of Supreme Court Justices and the Separation of Powers
1984-1985 M.A. Government, Claremont Graduate School
    Thesis: “Campaign Finance Reform: A Study in Unintended Consequences”
1978-1982 B.A. Political Science, California State University, San Bernardino

EMPLOYMENT
2010-Present Division Chair, University of Arizona, South
    Program Director for the Bachelor of Applied Sciences (BAS) core program, for the BAS in Cyber Operations, the BAS in Administration of Justice, and the BA in Government and Public Service. Created both the BAS in Administration of Justice and the BAS in Cyber Operations degree programs: developed the curriculum, obtained university approval, and implemented the programs. Created Undergraduate Certificates in Cyber Operations and in Cybersecurity. Directed the process for converting the BAS programs into fully online programs available in UA Online. Teach courses in American Government, national security policy, constitutional law, cyber law, policy, and ethics, immigration studies, political philosophy. Received the Superior Faculty award in 2014.

2012-2015 Associate Instructor of Political Science, Cochise College, Sierra Vista, Arizona
    Taught political science courses in American Government and U.S. and Arizona Constitutions.
2002-2014 Assistant Superintendent, Center for Academic Success Charter School District, Sierra Vista and Douglas, Arizona
Administered all state and federally-mandated educational programs, including special education programs, *No Child Left Behind* programs, testing and assessment, curriculum development, professional development, and grants and entitlements. Appointed member of two statewide policy-making committees: *No Child Left Behind* Committee of Practitioners, which approved educational policy under *No Child Left Behind* for the state of Arizona, and the Accountability Working Group, which approved educational policy under *Arizona Learns*, Arizona’s education accountability statute. Recruited and hired faculty and staff and supervised all staff training.

1998 Adjunct Professor of Political Science, State University of New York, Jefferson Community College
Taught Introductory Political Science to soldiers in the 10th Mountain Division-sponsored Higher Education Program.

1988-1997 Assistant Professor of Political Science, Tenured, Department of Political Science and National Security Studies, California State University, San Bernardino
Developed and taught lower and upper division and graduate courses for the Department of Political Science and National Security Studies, and the School of Social and Behavior Sciences. As Assistant Department Chair, scheduled courses, managed faculty assignments, monitored student enrollment, developed a student advising program and directed faculty recruitment. Served as chair of and member on numerous committees, including five years as chair of the school curriculum development committee. Served as advisor to numerous organizations both on and off campus. I attended conferences and presented papers on a wide variety of political, historical and philosophical issues. Provided analysis and commentary on a weekly radio program devoted to discussing current political issues. Advised a variety of student organizations, and served for seven years as Faculty Director of the student government corporation for the University. Received numerous awards for teaching excellence and university and community service and received the "Outstanding Faculty Award" my last three consecutive years at the University.

1985-1988 Research Assistant, Institute for Governmental Affairs and Teaching Assistant, Department of Political Science, University of California, Davis
Researched and wrote drafts on topics dealing with presidential politics, the war-making powers and the Vietnam War. Researched and wrote successful grant proposals, and planned and coordinated conferences and programs involving legislators, policy analysts, media commentators and scholars. Taught courses in Political Science, Political Philosophy, International Relations and Public Law. Received the "Outstanding Graduate Student Award for Teaching" for the 1987-1988 academic year.

1982-1985 Assistant Director, *Concilio* of Riverside County, California
Assisted in developing and administering a nonprofit economic development agency that contracted with federal, state and county agencies to provide employment programs, job training programs and employer incentive programs. Successfully lobbied public officials on behalf of the agency for
increased funding and programmatic authorization. Developed a public relations campaign to encourage prospective employers to relocate into the county. Supervised numerous employees, including job counselors, job training specialists and clerical staff and managed the day-to-day administration of the agency.

Recent Conference Presentations:


Cyber Security AAS Pathways, MCCCC Conference, Mesa, AZ, February 26, 2016.

“Ethics in Governance,” Third Annual Secular Summit, Phoenix, AZ, December 2, 2017
CURRICULUM VITAE

Chronology of Education

Ph.D., Computer Science, Brigham Young University, August 2003.
  Dissertation: Source Discovery and Schema Mapping for Data Integration.
  Advisor: David W. Embley.


M.S., Computer Science, University of Science & Technology of China, P.R.China, July 1997.
  Thesis: A Database System for Forest Fire Management.
  Advisors: Baohua Zhao and Qiangan Wang.

B.S., Computer Science, Shandong University, P.R.China, July 1994.

Chronology of Employment

Associate Professor, University of Arizona South, July 2009–Present

Assistant Professor, University of Arizona South, August 2003–June 2009

Research Assistant, Brigham Young University, August 1999–July 2003

Instructor, Brigham Young University, Spring 2002

Software Engineer, Defeng Company, Jinan, Shandong, P.R.China, October 1997–May 1998

Research Assistant, University of Science & Technology of China, P.R.China, September 1994–July 1997

Honors, Awards and Certificates

Certificate awarded for passing QM Peer Reviewer Course (PRC), 2017

Certificate awarded for passing Independent Applying the QM Rubric (APPQMR): (Statewide Systems), 2017.

Scholarship for Mid Career Mentoring Workshop by Computing Research Association Women (CRA-W), 2015

The 2013 Fall Superior Faculty Award, nominated and awarded by University of Arizona South faculty, sponsored by the University of Arizona South Foundation, 2014

Scholarship for Managing the Academic Career for Faculty Women at Undergraduate Computer Science and Engineering Institutions Workshop, 2007

Educator Scholarship for the 2005 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2005), 2005
Graduate Research Assistantships, Brigham Young University, 1999–2003
Graduate Tuition Scholarships, Brigham Young University, 1999–2003
Graduate Tuition Scholarship, University of Akron, 1998–1999
Graduate School Fellowship, University of Science & Technology of China, P.R.China, 1995–1996
Graduate Research Assistantships, University of Science & Technology of China, P.R.China, 1994–1997
Best Graduate Honor, Shandong University, P.R.China, 1994
Merit-based Scholarships, Shandong University, P.R.China, 1990–1993

Service/Outreach

Local/State Outreach

Participated as a mentor for Dev Day Yuma’s inaugural coding event on February 25, 2017
Participated in Dev Day Yuma Training sessions (four sessions) to serve as a faculty mentor for Dev Day Yuma’s inaugural coding event in January and February 2017
Participated in AWC/UASouth INSTINCT2 grant preparation and launching activities, Fall 2015—Present
Participated in developing Informatics and Computer Science major programs to transfer students from Arizona Western College at UA Yuma, Fall 2013–Present
Participated in offering UA South Mathematics and Computer Science minor programs to transfer students from Arizona Western College at UA Yuma, Fall 2012–Spring 2015
Participated in a Collaborative Partnership Showcase by Pima College East Campus and UA South, April 2015
Presented UA South Computer Science, Mathematics, and Informatics curricula to TASK Software Engineers and initiated collaboration, Fall 2013–Spring 2014
Examined Arizona Western College Informatics degree draft and shared the review with AWC Hispanic-Serving Institutions Science Technology Engineering & Mathematics and Articulation Programs proposal development committee, Fall 2013
Worked with faculty at Arizona Western College to develop pathways for CS minor and Informatics programs, Fall 2012
Participated in professional development activities on behalf of Southern Arizona Writing Project and i3 Grant Leadership Team, Fall 2012–Spring 2014
Participated in UA South and Cochise MACS (Mathematics and Computer Science) Club activities, Fall 2003–Present

Participated in Spring 2010 Welcome Back Bash, February 2010

Participated in Summer 2009 Online Teaching Group activities at UA main campus, Summer 2009

Participated in discussion about research collaboration with the ILEX Systems Arizona in 2007

Participated in “Cochise College Recruitment Days” on February 12, 2007

Participated in discussion about expanding recruitment of UA South CS graduates with the Oberon Associates, Inc in November 2006

Participated in discussion about expanding recruitment of UA South CS students with the JITC XML Lab in 2005

Participated in discussion about expanding recruitment of UA South CS students with the JDEP Operations Center of Northrop Grumman Mission Systems in March 2004

Participated in “Meetings with the Employer Day for participants in the H1B Technology Training Grant” on October 31, 2003

Participated in the articulation meeting in Computer Science/Computer Information Systems on October 3, 2003

National/International Outreach

Invited International Program Member for Computational Thinking Education 2018 (CTE2018)

Invited International Program Member for Computational Thinking Education 2017 (CTE2017)

Serve at the Editorial Board of the International Journal on E-Learning, Spring 2016–Present

Participated in CyberGen Denver Chinese Immersion Student Camp in Denver, Colorado on June 19-23, 2017

Participated in CyberGen Hawaii Teacher Camp in Honolulu, Hawaii on June 15-16, 2017


Participated in Mid Career Mentoring Workshop (Education, Research and Lab tracks) in Portland, Oregon on June 13-14, 2015

Member of Association for the Advancement of Computing in Education (AACE), 2015

Member of Association of Computing Machinery (ACM), 2008–Present
Invited referee for the Journal of Web Semantics, 2010

Member of IEEE, 2009–2010

PC member for the First International Workshop on Data Semantics in Social Computing Systems (DiSCo 2008)

PC member for the 2007 IRMA International Conference

PC member for the 25th International Conference on Conceptual Modeling (ER 2006)

PC member for the 2006 IRMA International Conference

PC member for the Seventh Asia Pacific Web Conference (APWeb 2005)

Invited referee for Information Processing Letters in 2008

Referee for evaluations of traveling scholarship applications to attend conferences of Grace Hopper Celebration of Women in Computing in 2008

Referee for the 2008 ACM SIGMOD International Conference on Management of Data (SIGMOD 2008)

Participated in the 39th ACM Technical Symposium on Computer Science Education (SIGCSE 2008)

Invited referee for the VLDB Journal in 2007

Participated in the 38th ACM Technical Symposium on Computer Science Education (SIGCSE 2007)

Participated in the Managing the Academic Career for Faculty Women at Undergraduate Computer Science and Engineering Institutions Workshop in 2007

Participated in the Learner-Center Education (LCE) workshops sponsored by the University of Arizona in September 2006 and January 2007

Chair of the Web Service Session of the 25th International Conference on Conceptual Modeling (ER 2006)

Participated in the Cultural Influence in the Classroom workshop in February 2005

Participated in the 2005 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2005)

Referee for the Fifth International Conference on Web Information Systems Engineering (WISE 2004)

Panelist of “Let’s get down to business: Mapping definition and discovery” at the Semantic Integration Workshop in the Second International Semantic Web Conference (ISWC 2003)
Referee for the Third International Conference on Web Information Systems Engineering (WISE 2002).
Referee for the 21st International Conference on Conceptual Modeling (ER 2002).
Referee for the 20th International Conference on Conceptual Modeling (ER 2001).
Referee for the Fourth International Workshop on the Web and Databases (WebDB 2001).
Referee for the 11th International Workshop on Research Issues on Data Engineering (RIDE 2001).
Referee for the 19th International Conference on Conceptual Modeling (ER 2000).
Volunteer worker for the 19th International Conference on Conceptual Modeling (ER 2000).

**Departmental and College Committees**

Program director and student major advisor of the Computer Science program at UA South, Fall 2003–Present

Program director and student major advisor of the Mathematics program at UA South, Fall 2009–Spring 2016

Program director and student major advisor of the Informatics program at UA South, Fall 2012–Present

Department liaison person to the Department of Mathematics at the UA main campus, Fall 2009–Spring 2016

Department liaison person to the Department of Computer Science at the UA main campus, Fall 2003–Present

UA South faculty co-advisor of MACS (Mathematics and Computer Science) club, Fall 2009–Present

Listserv Manager of UA South and Cochise CS Brown Bag Group, Fall 2003–Present

Member of two P&T Committees, Fall 2017

Chair of UA South Search Committee for Assistant Professor of Practice in Computer Science and Informatics, Spring 2017

Chair of UA South Search Committee for Program Director of Network Administration, Fall 2015–Spring 2016
Chair of UA South Network Administration Search Committee, Fall 2012–Spring 2013
Chair of UA South Curriculum Committee, Fall 2007–Spring 2009, August 2011–May 2013
Appointed leader of UA South STEM Working Group, October 2011-May 2012
Chair of UA South Personnel Committee, Fall 2010–Spring 2011, Fall 2015
Member of UA South Faculty Forum, Fall 2003–Present
Member of UA South Personnel Committee, Fall 2006–Spring 2010, Fall 2014–Present
Member of Education Technology Advisory Board, Fall 2013–Present
Member of UA South Curriculum Committee, Fall 2012–Spring 2014
Member of UA South Superior Faculty Committee, Fall 2014
Member of UA South P&T Committee, Fall 2013
Member of UA South Third-Year Review Committee, Fall 2010, Fall 2015
Member of UA South Dean’s Level Audit Committee, Fall 2009
Member of Search Committee to find an Academic Advising Coordinator, August 2012
Member of Continue Education Scholarship Committee, January 2012
Member of UA South ad-hoc committee to select student graduation speakers for Sierra Vista and Pima County Campuses, April 2006, April 2009, April 2010
Member of Northrop Grumman Scholarship Evaluation ad-hoc Committee at UA South, August 2004–Present
Member of UA South Recognition Committee, August 2007–May 2008
Member of UA South Education Technology Graduation Portfolio Defense Committee, April 2008
Member of UA South Curriculum Committee, August 2003–May 2007
Member of UA South Governance Committee, August 2003–May 2004

Other Committees (Internal or External)
Member of Southern Arizona Writing Project and i3 Grant Leadership Team, Fall 2012–Spring 2014

Publications/Creative Activity (Published or Accepted)
Peer-reviewed Journal Articles


Peer-reviewed Proceedings


1The * to the left of any publication title indicates that the research is based on work done as a graduate student.


Conference/Scholarly Presentations

Conference Presentations


Li Xu, *Learning Computational Thinking Online: A Student-Centered, Participatory Approach*, the 11th Annual Computer Science Education and Computer Science Conference (CSECS 2015), Boston, Massachusetts, June 4–7, 2015.


Colloquium Presentations

Li Xu, Flory Simon, and Lisa Holland. **Infusing Computational Thinking and Data Analysis for Teaching Improvement**, Southern Arizona Writing Project i3 Grant Bisbee High and Middle School Teacher Professional Development Retreat, February 2014.

Li Xu and Flory Simon, **Infusing Computational Thinking into Teaching Activities: How to Teach Writing Argumentative and Informational Text with Emphasis on the Common Core Standards**, Southern Arizona Writing Project i3 Grant Bisbee High School Teacher Professional Development Retreat, August 2013.

Li Xu, **The Power of Computational Thinking**, UA South Faculty Forum, January 16, 2013


Li Xu, **Object Oriented and 3D Programming in Alice**, UA South MACS Club, March 2012.

Li Xu, **3D Programming with Alice**, UA South MACS Club, March 2011.

Grants

Li Xu, Betul O. Czerkawski, John Delalla, University of Arizona OIA Grant for **Developing an Online Informatics Program**, January 2013. **Funded at $30K**, PI.

Li Xu, University of Arizona OIA Grant for **Converging Face-to-face and Online Learning Operating Systems in Computer Science**, November 2011. **Funded at $9941.85**, PI.

Curriculum Vitae

Odile Wolf
2222 E LA MADERA DR
Tucson, AZ 85719
tel: 520-576-7167
odile_wolf@hotmail.com

Education
1993-1998 University of Oregon PhD- ABD, Computer Science
1990-1992 Maharishi International University MS, Computer Science
1989-1990 Université Louis Pasteur (Strasbourg I) Licence, Computer Science

Additional Education and training:
2014 Accessibility MOOC 2014
2014 Quality Matters reviewer update
2013 Designing your blended course (QM)
2013 Quality Matters reviewer certification
2011 Applying the Quality Matters Rubric certification

Professional Experience:
Aug 2017 to present

Assistant Professor of Practice in Computer Science and Informatics,
University of Arizona South, Sierra Vista, AZ
- Taught classes in java, C, Databases, Algorithms, and Computational thinking and doing
- Taught online, blended and compressed classes
- Developed 5 online classes
Aug 2010 – May 2017

**Faculty for CS and CSA,** *Pima Community College, Tucson, AZ*
- Created 3 original classes in Android programming and 2 certificates
- Updated 10 existing classes curriculum
- Overhauled antiquated web programming certificate
- Initiated district wide book reviews
- Initiated collaborative effort for classes taught at various campuses
- Created 4 masters for online classes.
- Participated in College wide effort to create the self-study for Higher Learning Commission
- Participated in focused effort to create boot camps courses for networking boot camp
- Taught Online, Blended and Face to Face classes for beginning and advanced programming, data structures, C, android, computer applications, and introduction to computer science, as well as language specific classes.
- Initiated and negotiated new articulation agreements with the University of Arizona (February 2016- present)
- In the process of creating a new AA for transfer to the University of Arizona
- Developed OER material for online master courses
- Created new Digital and Information Literacy standards for the college (Sept 2016)
- Presented a lecture on “Microlectures” at the NW Tech Expo (March 2016)

2008-2010

**Adjunct Faculty in CS,** *Pima Community College, Tucson, AZ*
- Solely responsible for syllabi, and class structure. Taught online, blended and face to face.

April 1998 – January 2004

**Software Engineer II/III,** *Timberline (Sage) Software, Beaverton, OR*
Worked with a team of 2 to 17 people to develop shrink-wrap applications for property management and project management. Responsible for software performance, interaction with other in house applications, design documents, new feature definition and scoping, planning, client satisfaction issues, and defining milestones and schedules. Work with QA to maintain quality and respond to urgent issues coming from the field. Code new features, refactor and maintain existing C++ and C code on Windows XP, Windows NT, Windows 98, Windows ME, Window 2000 and Window XP using MFC technology and in-house UI.
1993-1998

**Research Assistant & Teaching Assistant, University of Oregon, Eugene, OR**
Performed research in the area of data mining, parallel debugging (state and event based), computer graphics, visualization, database, computer networks, software engineering, and computer ethics. Developed and taught courses in the areas of software engineering and object oriented programming for non-computer majors.

- Taught classes of up to 50 students. Teaching experience varied from teacher assistant to sole class responsibility, which required developing the syllabus and ordering books through posting grades.
  [http://www.cs.uoregon.edu/research/paracomp/publ/htbin/bibify.cgi?cmd=show&status=confirm&data_present=no&coll=CONF&id=spdt96](http://www.cs.uoregon.edu/research/paracomp/publ/htbin/bibify.cgi?cmd=show&status=confirm&data_present=no&coll=CONF&id=spdt96)

**Leadership Activity:**
July 2013 – May 2017

**Department Chair for East Campus Computer Science (CS) and Computer Science Application (CSA), Pima Community College (PCC), Tucson, AZ**
- Staff and manage all CIS, CSA, BUS, ACC adjunct faculty and classes
- Review all syllabi, classes
- Responsible for annual review for adjuncts.
- Includes online, blended and in person classes.
- Handle adjunct faculty-student conflicts

Jan 2014-May 2015

**Active member of the Online Education Task Forces Pima Community College (PCC), Tucson, AZ**
- Benchmarked other institutions online initiatives
- Surveyed and analyzed other institutions online faculty training, faculty and course oversight
- Developed solely or as a dyad most of the framework for Pima community college online campus including but not restricted to:
  - Online training framework
  - Teacher evaluation of online courses
  - Online department head responsibilities
  - QM review framework
- Wrote the Accessibility section used in the online faculty training
• Presented the effort information for approval to various groups including faculty senate
• Incorporated feedback from the groups into the framework

Feb 2012 – May 2015; Jan 2017-May 2017
Served as faculty representative to faculty senate, Pima Community College, Tucson, AZ
• As part of Criterion 5 (HLC), formalized the role of the newly created governing council
• Elected representative to two task forces charged by the chancellor to revamp the online education paradigm
• Defined the template for training Faculty, and Quality Assurance model for online and blended classes.

Aug 2011 – Aug 2014
Faculty Co-Chair for the CS and CSA College Discipline Area Committee
Pima Community College, Tucson, AZ
• Lead District wide change for two classes, including curriculum overhaul which impacted the college at large
• Defined direction for the CS and CSA Committee
• Encouraged a collaborative movement in a committee filled with strife

Aug 2010 – Aug 2014
Faculty Student Learning Outcome (SLO) Leader for the CS and CSA College Discipline Area Committee, Pima Community College, Tucson, AZ
• Lead definition of SLO for Computer Science and Computer Science Application
• Distributed SLO, gathered results and analyzed them.

Community involvement

2017-present Pima County Animal Care Center, Tucson AZ
2013-present Lend A hand (help to seniors), Tucson AZ
2012-present Divorce Recovery group leader, Tucson, AZ
2011-2017 Valley of the moon, Tucson, AZ
2001-2005 Big Brother, Big Sister, Portland OR
1998-2001 Portland Women Crisis Line volunteer and board member
1996-1998 Emergency Room volunteer, Sacred Heart hospital, Eugene, OR
Sandra Moore  
M.S., CISSP, CHFI, CCFE

E-mail smoore153@gmail.com  
Phone 702-343-0639

Summary  
I have lead projects, supervised and trained personnel on technical analysis procedures, briefed government and high-level clients on cyber threats, and conducted quality control on products prior to dissemination. I am looking for a senior level position, continue in a leadership role and continue to enhance my skills in the cyber arena.

Certifications:  
Certified Information Systems Security Professional (CISSP), July 2013  
Certified Hacking Forensic Investigator (CHFI), August 2012  
Certified Computer Forensics Examiner (CCFE), August 2012  
Security+, 2010

Education  
DSc Cybersecurity, Expected 2020  
Specialization: Cybersecurity  
Capitol Technology University, Laurel, MD

Master of Science, Graduated May 2012  
Major: Cyber Security: Intelligence/Forensics  
Utica College, Utica, NY

Bachelor of Science, Graduated August 2008  
Major: Cyber Security and Information Assurance, Emphasis in Computer Forensics  
Utica College, Utica, NY

Bachelor of Arts, Graduated December 2001  
Major: Media Arts, Emphasis in Production  
Minor: Criminal Justice  
University of Arizona, Tucson, AZ

Training  
Air Force Institute of Technology (AFIT)  
• Information warfare  
• Computer Network Attack and Defense

Wright-Patterson AFB, OH  
• Computer Exploit Development: Buffer Overflow/Stack Overflow

SANS Course: Advanced Digital Forensics and Incident Response

Employment  
Program Director  
Assistant Professor  
Network Administration  
University of Arizona South  
Member of National Cyber Watch Center’s Curriculum Standards Panel (NCC-CSP)

- Create/develop modern and up to date computer networking program  
- Develop advanced coursework to include the development of new courses in  
  - Cyber Intelligence, network, network security and digital forensics courses  
- Hire and oversee highly qualified Cyber Security Adjunct professors  
- Develop advanced course work in the Bachelor of Applied Science Cyber Operations program and BAS Network Administration
• Instruct and mentor students in cyber intelligence, computer networking, security and digital forensics
• Conduct community outreach throughout Arizona
• Attend President’s Cabinet meetings at local community colleges
• Promote diverse student body organizations and programs
• Instructor of Digital Forensics, Network Security, Network Administration, etc.

**Adjunct Professor Digital Forensics/Incident Response**  
Capitol Technology University  

January 2014-2016

- Instruct students on computer forensic investigations/incident response
- Provide detailed and real world experience regarding the forensic investigative process
- Create mock forensic investigations/labs to include the use of current digital forensics tools

**Lead Technologist Cyber Analyst**  
Booz Allen Hamilton  

October 2014- May 2016

- Serve as a network analyst as part of a Computer Network Operations (CNO) team, focusing on traffic analysis
- Perform passive fingerprinting techniques on network traffic to characterize physical and logical layout
- Conduct research and evaluate technical analysis with specific emphasis on network operations and tactics, techniques, and procedures
- Analyze network events to determine the impact on current operations and conduct research to determine capability and intent
- Produce high quality papers, presentations, recommendations, and findings for senior government officials
- Provide training to junior staff on tools, techniques, and procedures for conducting network traffic log analysis

**Sr. Intelligence Analyst, Defense Industrial Base CERT Officer (DCO)**  
October 2013-October 2014  
Defense Cyber Crime Center (DC3)  
General Dynamics Information Technology (GDIT)

- Lead and train incoming DIBCERT Analysts in an operations floor environment
- Determine product assignment for DIBCERT Analysts
- Conduct quality control analysis of all DIBCERT products prior to dissemination
- Disseminates publications to DIB Partners and US Government agencies
- Respond to Requests For Information (RFI)
- Continually provide process improvement of daily operations
- Provide end of day summary reports to the Director of DC3 and senior level government agencies
- Engage with cyber intelligence analyst counterparts across the US Intelligence and Law Enforcement communities
- Liaison with other DCISE cells and government agencies
- Periodically attend Branch Manager meetings
- Produce analytical reports for DIB Framework Agreement Partners, US Government Stakeholders, and other government partners that are responsible for providing computer network defense
- Provide indicators for defense in depth procedures to secure enterprise networks
- Produce products to include malware and forensic analysis for technical and non-technical individuals
- Apply knowledge of Advance Persistent Threat (APT) sets to enhance quality of reporting and correlate prior cyber events to provide a complete view of TTPs for each set
- Analyze event data and correlate information security threats from network data (proxy, firewall, IDS/IPS, router/switch logs and packet captures)
- Provide technically detailed cyber briefs to government and Defense Industrial Base clients
- Provide weekly activity report for DIBCERT operations to DCISE management
- Monitor Communication Portals and represent DC3/DCISE as a subject matter expert to DC3 Partners

**Intelligence Analyst**  
February 2013 - October 2013  
Defense Cyber Crime Center (DC3)  
General Dynamics Information Technology (GDIT)

- Respond to Requests For Information (RFI)
- Engage with cyber intelligence analyst counterparts across the US Intelligence and Law Enforcement communities
- Produce analytical reports for DIB Framework Agreement Partners, US Government Stakeholders, and other government partners that are responsible for providing computer network defense
- Provide indicators for defense in depth procedures to secure enterprise networks
- Produce products to include malware and forensic analysis for technical and non-technical individuals
- Apply knowledge of Advance Persistent Threat (APT) sets to enhance quality of reporting and correlate prior cyber events to provide a complete view of TTPs for each set
- Analyze event data and correlate information security threats from network data (proxy, firewall, IDS/IPS, router/switch logs and packet captures)
- Provide technically detailed cyber briefs to government and Defense Industrial Base clients
- Monitor Communication Portals and represent DC3/DCISE as a subject matter expert to DC3 Partners

**Computer Scientist**  
December 2011 - February 2013  
Department of the Air Force

- Analyze, produce and disseminate Cyber Threat Analysis products for government agencies
- Produce quarterly situational awareness reports regarding current cyber threats to the Air Force
- Maintain confidentiality and integrity of information systems
- Analyze forensic reports and collaborate with other government agencies on intrusion sets
- Conduct threat vector Analysis by correlating current cyber threats targeted towards the Department of Defense (DoD)
- Provide situational awareness to employees on physical safety measures, to include locations of fire extinguishers, AEDs, muster points and act as CPR instructor for military and civilian members
- Facilitate SharePoint, update product information and assist users

**Legal Office, Student Clerk**  
September 2010 – December 2011  
U.S. Customs and Border Protection

- Conduct e-Discovery and electronic based evidence gathering for trial preparation
- Implement encryption protocols/solutions to ensure confidentiality and integrity PII of staff members
- Deliver training to new clerks on procedures regarding confidentiality of PII and data according to the Freedom of Information Act (FOIA)
- Provide security services by logging and checking visitor identification prior to admittance
- Direct use of biometric software to record identifying information for purposes of authenticating staff members
- Process Federal Tort Claims and provide necessary documentation to petitioners
- Maintain database tracking system by Open/Close files, Upload Supporting Documentation
- Redact documents and process according to the Freedom of Information Act (FOIA) in order to maintain data integrity and confidentiality
- Archive Case files
- Create and update procedure manual for staff members
- Provide research/trial preparation assistance to the Assistant Chief Counsel and legal staff

**Nook e-Reader Support and Café Member**

*November 2009 - December 2010*

- Barnes & Noble
- Provide technical support for Nook e-Reader to include OS patches/updates/upgrades/troubleshooting
- Explain technical information to non-technical customers
- Secure and maintain equipment within a restricted and locked environment
- Electronic Sales
- Deploy products in timely manner

**Patient Care Technician**

*September 2008 - January 2010*

- El Dorado Urgent Care
- Update patient database and authenticate patient PII via insurance portal
- Maintain patient confidentiality and PII in a secure manner by
- Monitor and log entry into facility
- Maintain and inform patients and staff of HIPAA laws/regulations
- Assist Doctors and Nurses in the care of individuals
- Financial transactions/logging of transactions

**IT/IS Support Specialist**

*May 2008 - October 2008*

- US Geological Survey/University of Arizona
- Troubleshoot, provide client support and help-desk functions to staff members
- Install security patches onto client/staff computers and ensure systems remain up and running by monitoring current security bulletins for potential risk
- Install, configure, backup, maintain production server environments
- Linux/Unix configuration
- Configure RAID arrays
- Maintain weekly and monthly reports
- Assist with disposal of old equipment per DOD established procedures

**Barista**

*March 2008 - September 2008*

- Starbucks Coffee Company
- Assist customers in stressful environment
- Provide customer service and coffee-oriented knowledge
- Deploy products in timely manner

**Emergency Medical Technician**

*June 2004 - December 2007*

- Southwest Ambulance
- Provide emergency medical care to the sick and injured
- Maintain compliance of HIPPA and medical-legal aspects
- Provide and review HIPPA regulations to new hires and various training materials
- Provide exceptional customer service

**International Customer Service Representative**  
TeleTech  
September 2003 - June 2004

- Provide international customs information
- Provide technical support/assistance
- Provide detailed information on products that can and cannot be shipped

**Tools/Skills**  

**Honors**  
Best New Faculty of 2014 award
Diversity Leadership Award 2012
U.S. Customs and Border Protection Unit Citation for outstanding legal support 2010-2011
Deans Honor List 2007/2008
Hello Martin,

Our Cyber Engineering track requires that students have C Programming before we admit them. We prefer to see ECE175 or equivalent to fill that prerequisite due to the focus and delivery of the ECE175 course. My apologies if I did not clearly state that in our proposal. We do have a great working relationship with the ECE Department and they do already offer ECE175 to our incoming students. Below you will see an email from Dr. Bose supporting our proposal and his support for using ECE175.

Please let me know if you require any additional information.

Warmest Regards,

Jason
Jason Denno
Director, Cyber Operations
National Center of Academic Excellence - Cyber Operations (CAE-CO)
University of Arizona
jasondenno@email.arizona.edu
520-227-7203

On Jan 8, 2019, at 10:37 AM, Bose, Tamal - (tbose) wrote:

Jason,
I support your proposal. We will be glad to offer ECE 175 to your students.
-Tamal

Tamal Bose, Ph.D.
Professor and Department Head
Electrical and Computer Engineering
University of Arizona
1230 E. Speedway Blvd.
Tucson, AZ 85721-0104
Phone: (520) 621-6193
Email: tbose@email.arizona.edu
www.ece.arizona.edu
Hello Tamal,

Below is the email I referenced in my voicemail this morning. Our Cyber Engineering Track has a requirement for C Programming before we admit them. As I mentioned in my voicemail, we prefer to see ECE175 or equivalent fill that prerequisite due to the focus and delivery of your C Programming class. I will be sending an email to clarify that the prerequisite is C Programming….and that ECE175 is our preference….it is not mandatory.

Is there any chance that you could please respond to this email with your support so I can forward it along with my response back to the committee.

Warmest Regards,

Jason

Jason Denno
Director, Cyber Operations
National Center of Academic Excellence - Cyber Operations (CAE-CO)
University of Arizona
jasondenno@email.arizona.edu
520-227-7203

Begin forwarded message:

From: "Marquez, Martin - (martinmarquez)"
<martinmarquez@email.arizona.edu>
Subject: RE: Updated Cyber Operations New Academic Program Proposal
Date: January 7, 2019 at 4:30:24 PM MST
To: "Denno, Jason R - (jasondenno)"
<jasondenno@email.arizona.edu>, "Henley, Esther M - (ehenley)"
<ehenley@email.arizona.edu>, "Citera, Barbara W - (bwcitera)"
<bwcitera@email.arizona.edu>, "Denno, Linda Lee - (Idenno)"
<Idenno@email.arizona.edu>, "Wieland, Sarah J - (swieland)"
<swieland@email.arizona.edu>, "Xu, Li - (lxu)"
<lxu@email.arizona.edu>, "Straight, Ryan M - (ryanstraight)"
<ryanstraight@email.arizona.edu>
Cc: "Coonan, Pamela J - (coonan)"
<coonan@email.arizona.edu>, "Alfie, Fabian R - (alfie)"
<alfie@email.arizona.edu>

Hi all,
I hope you had a nice and relaxing holiday break.

I am writing to give you an update on the progress of the proposed BAS in Cyber Operations.

Associate Dean Jim Baygents, from the College of Engineering, sent a comment on 12/21/18:

“One quick comment about BAS CyberOps: it appears that entry into the Cyber Engineering subplan requires ECE 175. Tamal Bose, Dept Head for ECE, should have been asked for consent to use that course. Generally speaking, courses in the college of engineering are not available to non-engineering students. ECE makes ECE 175 available to non-engineers at ECE’s discretion.”

We would recommend that you reach out to Tamal Bose (tbose@email.arizona.edu), ECE Department Head, to request consent and obtain letter of support (or email) for using ECE 175. You can forward the memo/email and/or your response to me for inclusion on the proposal document.

Additionally:

The proposal was approved by CAAC and will next be considered during the 1/22/19 Academic Program Subcommittee (APS) meeting. The APS meeting is scheduled for 3:30-5:00pm in the Student Union- Santa Cruz Room. I estimate your presentation time to be 4:15pm. This is an estimation and may be earlier/later depending on proposals considered prior to your estimated time. Come prepared to present a ~5 minute summary and address any questions/comments from subcommittee members. Please let me know the name(s) of the presenter(s). Please wait outside the meeting room. I will come out to get you when the subcommittee is ready.

Approval stages remaining:
1. Jim Florian reviews the budget
2. Academic Program Subcommittee (APS; meets 1/22/19)
3. Undergraduate Council (UGC; 2/12/19 if approved at APS)
4. Provost Council (if approved at UGC; usually meets twice monthly)
5. Faculty Senate (last internal approval required; probably March 11, 2019; depends on above approvals)
6. Arizona Board of Regents (ABOR; proposal to be sent to ABOR for their February meeting)
Best,

Martin Marquez II  
Assistant Director for Academic Programs  
Office of Academic Affairs  
University of Arizona  
Curricular Affairs collaborates with and provides services for administrators, faculty, academic professionals, staff, and students to advance the academic mission of the University of Arizona.

From: Marquez, Martin - (martinmarquez)
Sent: Wednesday, December 12, 2018 1:01 PM
To: Denno, Jason R - (jasondenno) <jasondenno@email.arizona.edu>; Henley, Esther M - (ehenley) <ehenley@email.arizona.edu>; Citera, Barbara W - (bwcitera) <bwcitera@email.arizona.edu>; Denno, Linda Lee - (ldenno) <ldenno@email.arizona.edu>; Wieland, Sarah J - (swieland) <swieland@email.arizona.edu>
Subject: RE: Updated Cyber Operations New Academic Program Proposal

Hi all,

The proposal (attached) was uploaded to CAAC’s box for the December meeting. I sent CAAC an email to distribute the proposal to their departments, per the 10 day review period. Dr. Kim Jones, CAAC chair, is included in this email. Dr. Jones will work with you on a presentation time for CAAC’s 12/18/18 meeting.

Best,

Martin Marquez II  
Assistant Director for Academic Programs  
Office of Academic Affairs  
University of Arizona  
Curricular Affairs collaborates with and provides services for administrators, faculty, academic professionals, staff, and students to advance the academic mission of the University of Arizona.

From: Denno, Jason R - (jasondenno) <jasondenno@email.arizona.edu>
Sent: Tuesday, December 11, 2018 8:02 PM
To: Henley, Esther M - (ehenley) <ehenley@email.arizona.edu>; Citera, Barbara W - (bwcitera) <bwcitera@email.arizona.edu>; Denno, Linda Lee - (ldenno) <ldenno@email.arizona.edu>; Wieland, Sarah J - (swieland) <swieland@email.arizona.edu>; Marquez, Martin - (martinmarquez) <martinmarquez@email.arizona.edu>
Hello All,

Attached you will find the updated BAS in Cyber Operations New Academic Program Proposal documents on the new forms, as well as all requested additional information, changes, and documentation.

Please let me know if you require any additional information.

Warmest Regards,

Jason

Jason Denno
Director, Cyber Operations
National Center of Academic Excellence - Cyber Operations (CAE-CO)
University of Arizona
520-227-7203
jasondenno@email.arizona.edu
VALIDATE: COMPETITIVE LANDSCAPE

### PROJECT CRITERIA

<table>
<thead>
<tr>
<th>Validate</th>
<th>Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Nationwide</td>
</tr>
<tr>
<td>Degree Level</td>
<td>Bachelor's degree</td>
</tr>
<tr>
<td>Time Period</td>
<td>12/1/2017 - 11/30/2018</td>
</tr>
<tr>
<td>Selected Programs</td>
<td>Cyber/Electronic Operations and Warfare (29.0207)</td>
</tr>
<tr>
<td>Career Outcomes mapped to Selected Programs of Study</td>
<td></td>
</tr>
</tbody>
</table>

### OVERVIEW

<table>
<thead>
<tr>
<th></th>
<th>#</th>
<th>% Change (2013-2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degrees Conferred</td>
<td>65</td>
<td>100%</td>
</tr>
<tr>
<td>Number of Institutions</td>
<td>6</td>
<td>100%</td>
</tr>
<tr>
<td>Average Conferrals by Institution</td>
<td>11</td>
<td>100.00%</td>
</tr>
<tr>
<td>Median Conferrals by Institution</td>
<td>4</td>
<td>100.00%</td>
</tr>
</tbody>
</table>
### MARKET SHARE BY PROGRAM

**Cyber/Electronic Operations and Warfare (100%)**

<table>
<thead>
<tr>
<th>Program</th>
<th>Conferrals (2017)</th>
<th>Market Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber/Electronic Operations and Warfare</td>
<td>65</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

### MARKET SHARE BY INSTITUTION TYPE
Institution Type

<table>
<thead>
<tr>
<th>Institution Type</th>
<th>Conferrals (2017)</th>
<th>Market Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>18</td>
<td>27.69%</td>
</tr>
<tr>
<td>Public</td>
<td>47</td>
<td>72.31%</td>
</tr>
</tbody>
</table>

TOP 10 INSTITUTIONS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>United States Naval Academy</td>
<td>Public</td>
<td>69.23%</td>
<td>69.23%</td>
<td>45</td>
<td>100.00%</td>
</tr>
<tr>
<td>Maryville University of Saint Louis</td>
<td>Private</td>
<td>16.92%</td>
<td>16.92%</td>
<td>11</td>
<td>100.00%</td>
</tr>
<tr>
<td>Fontbonne University</td>
<td>Private</td>
<td>6.15%</td>
<td>6.15%</td>
<td>4</td>
<td>100.00%</td>
</tr>
<tr>
<td>Thomas College</td>
<td>Private</td>
<td>4.62%</td>
<td>4.62%</td>
<td>3</td>
<td>100.00%</td>
</tr>
</tbody>
</table>
### TOP 10 PROGRAMS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber/Electronic Operations and Warfare</td>
<td>100.00%</td>
<td>100.00%</td>
<td>65</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

### ACTIVE COMPETITORS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern Michigan University</td>
<td>Public</td>
<td>3.08%</td>
<td>3.08%</td>
<td>2</td>
<td>100.00%</td>
</tr>
<tr>
<td>Excelsior College</td>
<td>Private</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>0.00%</td>
</tr>
</tbody>
</table>